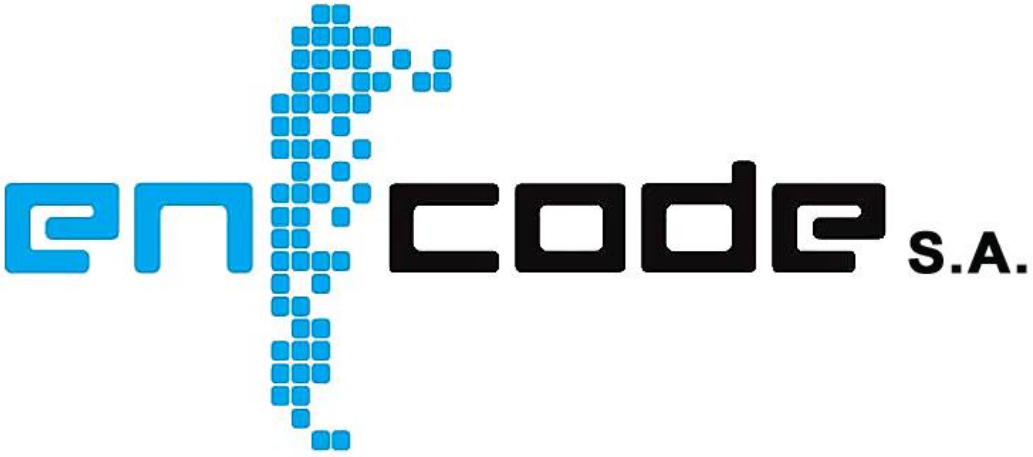

POLÍTICA ÚNICA DE CERTIFICACIÓN DE ENCODE S. A.

VERSIÓN 4.1 – FECHA 25/09-/2021

CLASE: PÚBLICO

DI-2021-109964170-APN-SSIA#JGM

VERSIONES Y MODIFICACIONES DE ESTE DOCUMENTO

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	2014/11/10	GrupoFD	Directorio ENCODE	Aprobación para presentación
2	0	2019/22/10	GrupoFD	Directorio ENCODE	Adecuación Resolución 399 E/2016
3	0	2020/11/11	GrupoFD	Directorio ENCODE	Adecuación normativa y servicio de custodia
4	0	2021/03/15	GrupoFD	Directorio ENCODE	Aprobación para presentación
4	1	2021/09/25	GrupoFD	Directorio ENCODE	Adecuación para sellos de competencia

ÍNDICE

1. INTRODUCCION 8
1.1 Descripción general 8
1.2 Nombre e Identificación del Documento 8
1.3 Participantes 8
1.3.1 Certificador 9
1.3.2 Autoridad de Registro 9
1.3.3 Suscriptores de certificados 9
1.3.4 Terceros Usuarios 10
1.4 Uso de los certificados 10
1.5 Administración de la Política 10
1.5.1 Responsable del documento 10
1.5.2 Contacto 10
1.5.3 Procedimiento de aprobación de la Política de Certificación 11
1.6 Definiciones y Acrónimos 11
1.6.1 Definiciones 11
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 16
2.4 Controles de acceso a la información 16
3. IDENTIFICACIÓN Y AUTENTICACIÓN 17
3.1 Asignación de nombres de suscriptores 17
3.1.1 Tipos de Nombres 17
3.1.2 Necesidades de Nombres Distintivos 17
3.1.3 Anonimato o uso de seudónimos 22
3.1.4 Reglas para la interpretación de nombres 23
3.1.5 Unicidad de nombres 23
3.1.6 Reconocimiento, autenticación y rol de las marcas registradas 23
3.2 Registro inicial 24
3.2.1 Métodos para comprobar la titularidad del par de claves. 24
3.2.2 Autenticación de la identidad de Personas Jurídicas Públicas o Privadas. 26
3.2.3 Autenticación de la identidad de Personas Humanas 30

7

3.2.4 Información no verificada del suscriptor. 31
3.2.5 Validación de autoridad. 31
3.2.6 Criterios para la interoperabilidad. 32
3.3 Identificación y autenticación para la generación de nuevo par de claves (Rutina de Re Key). 32
3.3.1 Renovación con generación de nuevo par de claves (Rutina de Re Key) 32
3.3.2 Generación de UN (1) certificado con el mismo par de claves 33
3.4 Requerimiento de revocación. 33
4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS 34
4.1 Solicitud de certificado. 34
4.1.1 Solicitantes de certificado. 34
4.1.2 Solicitud de certificado. 35
4.2 Procesamiento de la solicitud del certificado 40
4.3 Emisión del certificado 42
4.3.1 Proceso de emisión del certificado 42
4.3.2 Notificación de emisión 43
4.4 Aceptación del certificado 43
4.5 4.5. Uso del par de claves y del certificado 44
4.5.1 Uso de la clave privada y del certificado por parte del suscriptor 44
4.5.2 Uso de la clave pública y del certificado por parte Terceros Usuarios 45
4.6 Renovación del certificado sin generación de un nuevo para de claves 45
4.7 Renovación del certificado con generación de un nuevo para de claves 45
4.8 Modificación del certificado 46
4.9 Suspensión y Revocación de Certificados 46
4.9.1 Causas de revocación 46
4.9.2 Autorizados a solicitar la revocación 47
4.9.3 Procedimientos para la solicitud de revocación 48
4.9.4 Plazo para la solicitud de revocación 49
4.9.5 Plazo para el procesamiento de la solicitud de revocación 49
4.9.6 Requisitos para la verificación de la lista de certificados revocados 49
4.9.7 Frecuencia de emisión de listas de certificados revocados 50
4.9.8 Vigencia de la lista de certificados revocados 50
4.9.9 Disponibilidad del servicio de consulta sobre revocación y de estado del certificado 50
4.9.10 Requisitos para la verificación en línea del estado de revocación 51

7

4.9.11 Otras formas disponibles para la divulgación de la revocación. 51
4.9.12 Requisitos específicos para casos de compromiso de claves 51
4.9.13 Causas de suspensión 51
4.9.14 Autorizados a solicitar la suspensión 51
4.9.15 Procedimientos para la solicitud de suspensión 52
4.9.16 Límites del periodo de suspensión de un certificado 52
4.10 Estado del certificado 52
4.10.1 Características técnicas 52
4.10.2 Disponibilidad del servicio 52
4.10.3 Aspectos operativos 52
4.11 Desvinculación del suscriptor 53
4.12 Recuperación y custodia de claves privadas 53
5. CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN 53
5.1 Controles de seguridad física 53
5.2 Controles de Gestión 54
5.3 Controles de seguridad del personal 54
5.4 Procedimientos de Auditoría de Seguridad 55
5.5 Conservación de registros de eventos 55
5.6 Cambio de claves criptográficas 56
5.7 Plan de respuesta a incidentes y recuperación ante desastres 57
5.8 Plan de Cese de Actividades 57
6. CONTROLES DE SEGURIDAD TÉCNICA 58
6.1 Generación e instalación del par de claves criptográficas 58
6.1.1 Generación del par de claves criptográficas 58
6.1.2 Entrega de la clave privada 60
6.1.3 Entrega de la clave pública al emisor del certificado 60
6.1.4 Disponibilidad de la clave pública del certificador 60
6.1.5 Tamaño de claves 61
6.1.6 Generación de parámetros de claves asimétricas 61
6.1.7 Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v.3) 61
6.2 Protección de la clave privada y controles sobre los dispositivos criptográficos 62
6.2.1 Controles y estándares para dispositivos criptográficos 62
6.2.2 Control "M de N" de clave privada 63
6.2.3 Recuperación de clave privada 63

6.2.4 Copia de seguridad de clave privada 63
6.2.5 Archivo de clave privada 64
6.2.6 Transferencia de claves privadas en dispositivos criptográficos 64
6.2.7 Almacenamiento de claves privadas en dispositivos criptográficos 64
6.2.8 Método de activación de claves privadas 64
6.2.9 Método de desactivación de claves privadas 65
6.2.10 Método de destrucción de claves privadas 65
6.2.11 Requisitos de los dispositivos criptográficos 65
6.3 Otros aspectos de administración de claves 66
6.3.1 Archivo permanente de la clave pública 66
6.3.2 Período de uso de clave pública y privada 66
6.4 Datos de activación 66
6.4.1 Generación e instalación de datos de activación 66
6.4.2 Protección de los datos de activación 67
6.4.3 Otros aspectos referidos a los datos de activación 67
6.5 Controles de seguridad informática 68
6.5.1 Requisitos Técnicos específicos 68
6.5.2 Requisitos de seguridad computacional 69
6.6 Controles Técnicos del ciclo de vida de los sistemas 69
6.6.1 Controles de desarrollo de sistemas 70
6.6.2 Controles de gestión de seguridad 70
6.6.3 6Controles de seguridad del ciclo de vida del software 70
6.7 Controles de seguridad de red 70
6.8 Certificación de fecha y hora 71
6.9 Servicio de emisión de Sello de Competencia y/o Atributo 71
7. PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS 72
7.1 Perfil del certificado 72
7.1.1 Número de versión 80
7.1.2 Extensiones 80
7.1.3 Identificadores de algoritmos 82
7.1.4 Formatos de nombre 82
7.1.5 Restricciones de nombre 82
7.1.6 OID de la Política de Certificación 82

7

7.1.7 Sintaxis y semántica de calificadores de Política 83
7.1.8 Semántica de procesamiento para extensiones críticas 83
7.2 Perfil de la lista de certificados revocados 83
7.2.1 Número de versión 84
7.2.2 Extensiones de CRL (Lista de Certificados Revocados) 84
7.3 Perfil de la consulta en línea del estado del certificado 84
7.3.1 Consultas OCSP 85
7.3.2 Respuestas OCSP 85
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 87
9. ASPECTOS LEGALES Y ADMINISTRATIVOS 88
9.1 Aranceles 88
9.2 Responsabilidad Financiera 89
9.3 Confidencialidad 89
9.3.1 Información confidencial 90
9.3.2 Información no confidencial 91
9.3.3 Responsabilidades de los roles involucrados 91
9.4 Privacidad 91
9.5 Derechos de Propiedad Intelectual 92
9.6 Responsabilidades y garantías 92
9.7 Deslinde de responsabilidad 94
9.8 Limitaciones a la responsabilidad frente a terceros 95
9.9 Compensaciones por daños y perjuicios 95
9.10 Condiciones de vigencia 95
9.11 Avisos personales y comunicaciones con los participantes 96
9.12 Gestión del ciclo de vida del documento 96
9.12.1 Procedimientos de cambio 97
9.12.2 Mecanismo y plazo de publicación y notificación 97
9.12.3 Condiciones de modificación del OID 98
9.13 Procedimientos de resolución de conflictos 98
9.14 Legislación aplicable 99
9.15 Conformidad con normas aplicables 99
9.16 Cláusulas adicionales 99
9.17 Otras cuestiones generales 99

1. INTRODUCCION

1.1 Descripción general

El presente documento establece las políticas que se aplican a la relación entre ENCODE S.A. en su carácter de certificador licenciado y los solicitantes, suscriptores y terceros usuarios de los certificados que éste emita, en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley N° 25.506 y sus modificatorias). Un certificado vincula los datos de verificación de firma digital de una persona humana o jurídica o con una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

La Autoridad de Aplicación de la Infraestructura de firma digital antes mencionada es la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, siendo dicho organismo y la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA, quienes conforman y entienden en las funciones de Ente Licenciante.

1.2 Nombre e Identificación del Documento

Nombre:	Política Única de Certificación de ENCODE S. A.
Versión:	4.1
Fecha:	25/09/2021
URL:	http://www.encodesa.com.ar/pu/ENCODEPU.pdf
OID:	2.16.32.1.1.4
Lugar:	República Argentina

1.3 Participantes

Integran la infraestructura del certificador las siguientes entidades:

1.3.1 Certificador

Razón Social: ENCODE S. A. CUIT: 30-71110353-4

Domicilio: Arturo M. Bas 34 Local PB - X5000KLB – Córdoba – Provincia de Córdoba

Teléfono: +54 (351) 569-4407 o 569-4408 y líneas rotativas

Sitio web: http://www.encodesa.com.ar

1.3.2 Autoridad de Registro

El certificador posee una estructura de Autoridades de Registro cuya información se encuentra disponible en:

- **http://www.encodesa.com.ar/autoridad-de-registro**

Contacto: Responsable de la Autoridad de Registro Central

Domicilio: Arturo M. Bas 34 Local PB - X5000KLB – Córdoba – Provincia de Córdoba

E-mail: arc@encodesa.com.ar

Teléfono: +54 (351) 569-4407 o 569-4408 y líneas rotativas

Sitio web: http://www.encodesa.com.ar/autoridad-de-registro

1.3.3 Suscriptores de certificados

Según los términos de la presente Política Única de Certificación, se define la Comunidad de Suscriptores de certificados digitales a todas las personas humanas o jurídicas de naturaleza pública o privada o responsables autorizados de aplicaciones y sitios seguros, que suscriban certificados de firma digital o provisión de servicios vinculados de firma digital con ENCODE S.A.

ENCODE S.A. es suscriptora de un certificado, para ser usado en relación con el servicio OCSP de consultas sobre el estado de los certificados.

1.3.4 Terceros Usuarios

Son terceros usuarios de los certificados emitidos bajo la presente Política Única de Certificación toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo a la normativa vigente. 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 de los certificados digitales emitidos bajo la presente Política Única de Certificación, podrán ser utilizadas por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, pudiendo ser empleadas para cualquier uso o aplicación, como así también para autenticación o cifrado.

1.5 Administración de la Política

1.5.1 Responsable del documento

Para realizar preguntas, efectuar reclamos o enviar sugerencias referidos al presente documento, el interesado deberá dirigirse a:

Contacto: Responsable de la Autoridad de Registro Central

Domicilio: Arturo M. Bas 34 Local PB - X5000KLB – Córdoba – Provincia de Córdoba

E-mail: mda@encodesa.com.ar

Teléfono: +54 (351) 569-4407 o 569-4408 y líneas rotativas

Sitio web: https://www.encodesa.com.ar/autoridad-de-registro

1.5.2 Contacto

El responsable del registro, mantenimiento e interpretación de la Política Única de Certificación es ENCODE SA.

Contacto: Responsable de la Autoridad de Registro Central

Domicilio: Arturo M. Bas 34 Local PB - X5000KLB – Córdoba – Provincia de Córdoba

E-mail: mda@encodesa.com.ar

Teléfono: 54 (351) 569-4407 o 569-4408 y líneas rotativas Sitio web: https://www.encodesa.com.ar/contacto

1.5.3 Procedimiento de aprobación de la Política de Certificación

El presente documento es la Política Única de Certificación de ENCODE S.A. OID 2.16.32.1.1.4 de conformidad con la Ley Nº 25.506, su Decreto Reglamentario Nº 182/2019 y modificatorios, la Resolución N° 86/2020 de la SECRETARÌA DE INNOVACIÓN PÚBLICA y la Resolución 946/2021 de la SECRETARÍA DE INNOVACIÓN PÚBLICA perteneciente a la JEFATURA DE GABINETE DE MINISTROS.

Esta Política Única de Certificación ha sido presentada ante el Ente Licenciante y ha sido aprobada por el correspondiente acto administrativo.

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

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

Autoridad de Aplicación: La SECRETARÌA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.

Autoridad de Registro: Es la entidad que tiene a su cargo las funciones de:

- Recepción de las solicitudes de emisión de certificados.
- Validación de la identidad y autenticación de los datos de los titulares de certificados.
- Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.

- Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
- Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
-
- Identificación y autenticación de los solicitantes de revocación de certificados.
- Archivo y la conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil, debiendo observar el procedimiento previsto para su funcionamiento como tal.

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

Autoridad de Sello de Competencia: Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.

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

Certificados de aplicaciones: definidos como aquellos que tienen la finalidad de identificar a la aplicación o servicio que firma documentos digitales o registros en forma automática mediante un sistema informático programado a tal fin. Los certificados digitales que permitan identificar en forma fehaciente en internet o cualquier otra red informática, a los servidores que establezcan conexiones seguras, son también certificados de aplicaciones.

Infraestructura tecnológica del Certificador Licenciado: Conjunto de servidores y otros equipamientos informáticos relacionados, software y dispositivos criptográficos utilizados para la generación, almacenamiento y publicación de los certificados digitales, y para la provisión de información sobre su estado de validez y para la prestación de otros servicios en relación a la firma digital enumerados en el Artículo 4 de la Resolución N°946/2021. La infraestructura tecnológica que soporta los servicios del certificador utilizada tanto en el establecimiento principal como en el alternativo destinado a garantizar la continuidad de sus operaciones, deberá estar situada en territorio argentino, bajo el control del certificador licenciado y afectada a tareas específicas propias de certificación, de custodia centralizada de claves privadas y demás servicios asociados a firma digital.

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

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).

Ente licenciante: La SECRETARÌA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS y la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA constituyen el Ente Licenciante.

Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL).

Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS).

Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

Plan de Contingencia: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.

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

Servicio OCSP (Protocolo en línea del estado de un certificado – "Online Certificate Status Protocol"): servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). 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 humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

Servicio de Firma Digital con Custodia Centralizada de Clave Criptográficas: Servicio que permite la generación y la realización del proceso de firma digital, el que operará utilizando un sistema técnicamente confiable y seguro conforme los lineamientos de la Ley N° 25.506 y modificatorias, cumpliendo con las normas de seguridad acordes a estándares internacionales y de auditoría establecidas por la Autoridad de Aplicación.

1.6.2 Acrónimos

ACR-RA: Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.

CRL: Lista de Certificados Revocados ("Certificate Revocation List"). **CUIT:** Clave Única de Identificación Tributaria.

DNFDIT: Dirección Nacional de Firma Digital e Infraestructura Tecnológica.

IEC: International Electrotechnical Commission.

IETF: Internet Engineering Task Force.

MM: Ministerio de Modernización.

SIP: Secretaría De Innovación Pública.

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

7

OID: Identificador de Objeto ("Object Identifier").

RFC: Request for Comments.

SMA: Secretaría de Modernización Administrativa.

SSIA: Subsecretaria de Innovación Administrativa.

2. RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS

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

2.1 Repositorios

Los repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por ENCODE S. A.

2.2 Publicación de información del certificador

El certificador ENCODE S. A. garantiza el acceso a la información de los siguientes documentos:

a) Política Única de Certificación.

b) Acuerdo Tipo con suscriptores.

c) Términos y condiciones con terceros usuarios ("relying parties").

d) Política de Privacidad.

e) Manual de Procedimientos

f) Información relevante de los informes de su última auditoría

g) Repositorio de certificados revocados

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

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

j) Listado de Autoridades de Registro (indicando si opera bajo modalidad móvil).

La publicación de información del Certificador Licenciado ENCODE S. A. se realiza en sus servidores, y se puede encontrar en el sitio web identificado como:

- **http://www.encodesa.com.ar/firma-digital**

Se mantiene el repositorio en línea accesible durante las VEINTICUATRO (24) horas, los SIETE (7) días de la semana.

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.

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

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

ENCODE S.A. garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

7

3. IDENTIFICACIÓN Y AUTENTICACIÓN

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

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 Necesidades 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): se corresponde con el nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.

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

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

"serialNumber" (OID 2.5.4.5: Nro. de serie): se encuentra presente y contiene el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o

aplicación, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

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

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

"countryName" (OID 2.5.4.6: Código de país): se encuentra presente y representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de **Persona humana:**

"commonName" (OID 2.5.4.3: Nombre común): se encuentra presente y corresponde con el nombre que figura en el Documento de Identidad del suscriptor.

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

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

En caso de ciudadanos argentinos o residentes: "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral.

En caso de extranjeros:

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

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

"countryName" (OID 2.5.4.6: Código de país): se encuentra presente y representa 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): Coincide 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): contiene 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): para certificados de aplicaciones, coincide con la denominación de la Persona Jurídica Pública o Privada.

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

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

a) "CUIT": Clave única de identificación tributaria para las Personas Jurídicas argentinas.

b) "ID" [país]: Número de identificación tributario para Personas Jurídicas extranjeras. El atributo [país] se encuentra codificado según el estándar [ISO3166] de 2 caracteres.

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

Para los certificados de sitio seguro:

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

"organizationalUnitName" (OID 2.5.4.11: Nombre de la Suborganización): contiene 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): se encuentra presente y contiene el nombre de la Persona Jurídica Pública o Privada responsable del sitio web.

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

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

"countryName" (OID 2.5.4.6: Código de país): se encuentra presente y contiene el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS

(2) caracteres.

7

Para los Certificados de Autoridad de Sello de Tiempo.

"commonName" (OID 2.5.4.3: Nombre común): se encuentra presente y contiene el nombre del servicio.

"organizationalUnitName" (OID 2.5.4.11: Nombre de la suborganización): contiene 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): coincide con la denominación de la Persona Jurídica Pública o Privada.

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

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

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

b) "ID" [país]: Número de identificación tributaria para Personas Jurídicas extranjeras. El atributo [país] está codificado según el estándar [ISO 3166] de DOS (2) caracteres.

"countryName" (OID 2.5.4.6: Código de país): está presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los Certificados de Autoridad de Sello de Competencia:

"commonName" (OID 2.5.4.3: Nombre común): está presente y contiene el nombre de la Autoridad de Competencia.

"organizationalUnitName" (OID 2.5.4.11: Nombre de la suborganización): contiene 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): coincide con la denominación de la Persona Jurídica Pública o Privada.

"serialNumber" (OID 2.5.4.5: Nro de serie): se encuentra presente y contiene el número de identificación 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]".

El valor posibles 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):): está presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

3.1.3 Anonimato o uso de seudónimos

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

7

3.1.4 Reglas para la interpretación de nombres

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

3.1.5 Unicidad de nombres

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

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

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

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

3.2 Registro inicial

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

El certificador cumple con lo establecido en:

a) El artículo 21, inciso a) de la Ley de Firma Digital Nº 25.506, el artículo 21, inc.7 del Anexo al Decreto Nº 182/2019, y el artículo 15 de la Resolución 946/2021 de la SECRETARÍA DE INNOVACIÓN PÚBLICA perteneciente a la JEFATURA DE GABINETE DE MINISTROS relativos a la información a brindar a los solicitantes.

b) El artículo 14, inciso b) de la Ley de Firma Digital Nº 25.506 relativo a los contenidos mínimos de los certificados.

c) El artículo 16 de la Resolución 946/2021 de la SECRETARÍA DE INNOVACIÓN PÚBLICA perteneciente a la JEFATURA DE GABINETE DE MINISTROS, relativo al consentimiento del solicitante para la emisión de certificados.

3.2.1 Métodos para comprobar la titularidad del par de claves.

El certificador comprueba que el solicitante se encuentra en posesión de la clave privada mediante la verificación de la solicitud del certificado digital en formato PKCS#10, la cual 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.

Para la comprobación de la posesión de la clave privada se utiliza el siguiente procedimiento:

- El Solicitante tiene a cargo la generación de su par de claves criptográficas asimétricas. Las claves criptográficas no quedan almacenadas en los sistemas informáticos de la AC de ENCODE S.A.

- Durante el proceso de solicitud, se requiere que el Solicitante realice la generación de un par de claves criptográficas asimétricas, dicha operación será realizada desde el equipo del solicitante y en ningún momento de la generación los sistemas informáticos de ENCODE S.A. tienen contacto con la clave privada del solicitante.

- En los casos en los cuales el Solicitante utilice una implementación por software para la generación del par de claves criptográficas asimétricas, la clave privada podrá quedar almacenada en su perfil de usuario o de la aplicación.

- En los casos en que el Solicitante utilizara un dispositivo criptográfico, las claves son generadas y almacenadas en él.

- Los datos de la Solicitud y el requerimiento con la clave pública del Solicitante, en formato PKCS#10, son enviados a la aplicación del Certificador.

- La aplicación del Certificador valida el requerimiento PKCS#10.

- En caso de ser correcto el formato, la aplicación del Certificador entrega al Solicitante una Solicitud completa incluyendo el resumen criptográfico.

- El Solicitante debe hacer entrega de la Solicitud a la Autoridad de Registro en el proceso de identificación, demostrando así la posesión de la clave privada.

- En los casos en que el Solicitante utilizara un servicio de firma digital con custodia centralizada de claves criptográficas, las claves son generadas y utilizadas en un dispositivo criptográfico FIPS 140-2 nivel 3.

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 se efectuará 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) validará 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 será verificada mediante documentación que acredite su condición de tal.

El certificador cumple con las siguientes exigencias reglamentarias impuestas por:

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

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

7

c) El artículo 21, inc.14 del Anexo al Decreto Reglamentario Nº 182/2019 relativo a la protección de datos personales.

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

Se conserva 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 firma UN (1) acuerdo que contiene la confirmación de que la información incluida en el certificado es correcta.

El Solicitante del certificado para persona jurídica debe haber completado el requerimiento de solicitud de certificado y creado el par de claves criptográficas, conforme "4.1.2.- Solicitud de certificado" y, previo pago del arancel correspondiente, se presentará en la AR seleccionada, con la documentación detallada en la "Guía del Solicitante", que se encuentra publicada en el sitio web: http://www.encodesa.com.ar/firma-digital/

El representante legal, apoderado o administrador de la persona jurídica Solicitante del certificado se presenta ante el Oficial de Registro con los documentos que se detallan más abajo con copias certificadas por Escribano Público los que correspondieren, tal cual se indica en la Guía del Solicitante:

a) Estatuto o Contrato Social correspondiente a la Persona Jurídica,

b) Acta de directorio o documento que acredite la representación invocada y su documento de identidad,

c) Constancia de inscripción en el Registro Público de Comercio,

d) Constancia de inscripción en AFIP,

e) DNI de todos los socios, en caso de sociedades irregulares,

f) Acta de distribución de cargos,

g) Poder General Amplio o Poder especial que autoriza la solicitud de certificado de firma digital. Se hace saber al Solicitante que se encuentra en la "Guía del Solicitante" el modelo de poder especial requerido a los fines de solicitar un certificado de firma digital,

h) Solicitud de certificado impresa,

i) Recibo que acredita el pago del certificado correspondiente,

j) A los fines de que el Solicitante tome conocimiento de la documentación que requiere ser acompañada para su identificación y la identificación de la persona jurídica que representa, se sugiere consultar la "Guía del Solicitante" que se encuentra publicada en el sitio web: http://www.encodesa.com.ar/firma-digital/

El Solicitante será atendido por un Oficial de Registro, quien verificará su identidad, la documentación que presenta y el resumen criptográfico vinculado con la Solicitud, así como toda otra información contenida en la Solicitud.

Una vez que fueron verificados los datos del suscriptor, se procede a realizar el reconocimiento físico, donde el oficial de registro debe tomar una foto de frente a la persona con la suficiente claridad para corroborarla con la que aparece en la fotocopia del DNI (documentación presentada). Luego se deberá registrar una huella digital para lo cual se le indica que en un lector de huellas coloque el mismo dedo CUATRO (4) veces seguidas. El sistema valida que realmente se cumplan estas CUATRO (4) veces, para poder continuar con el procedimiento de reconocimiento que tiene por finalidad dejar asociado al certificado una foto y una huella dactilar representativa de la persona.

Si la identificación ha sido satisfactoria, el Solicitante firma dos ejemplares impresos del "Acuerdo con Suscriptores", quedando uno en poder del Solicitante y el otro en poder de la Autoridad de Registro correspondiente.

7

El Oficial conserva para el armado de la carpeta del suscriptor la documentación presentada como respaldo del proceso de identificación.

Recibida la documentación en la AR, el Oficial de Registro procederá a efectuar el control de la documentación. Luego cargará en la aplicación de la Autoridad de Registro la confirmación de los documentos recibidos y determinará la aceptación o rechazo de la Solicitud.

En caso de aprobar la Solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.

Finalmente, en caso de aprobación, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona jurídica Solicitante. Esta contiene la Solicitud de Certificado, y todos los documentos presentados de acuerdo a lo exigido en la "Guía del Solicitante" y el Acuerdo con Suscriptores firmado.

Si la Solicitud es rechazada o dada de baja por falta de identificación, la aplicación le informará la condición al Solicitante por medio de un correo electrónico.

Para los casos de renovación, la Autoridad de Registro podrá requerir, ante dudas respecto de la verificación realizada con anterioridad, que el Solicitante/Suscriptor se presente nuevamente para acreditar identidad.

En caso de solicitudes de certificados para sitios seguros se identificará al suscriptor a cuyo nombre ha sido registrado un dominio DNS y al responsable autorizado del suscriptor

3.2.3 Autenticación de la identidad de Personas Humanas

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

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

- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.
- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.
- Una vez que fueron verificados los datos del suscriptor, se procede a realizar el reconocimiento físico, donde el Oficial de Registro debe tomar una foto de frente a la persona con la suficiente claridad para corroborar con la que aparece en la fotocopia del DNI (documentación presentada). Luego se deberá registrar una huella digital para lo cual se le indica que en un lector de huellas coloque el mismo dedo CUATRO (4) veces seguidas. El sistema valida que realmente se cumplan estas CUATRO (4) veces, para poder continuar con el procedimiento de reconocimiento que tiene por finalidad dejar asociado al certificado una foto y huella dactilar de la persona.

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 Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

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

7

c) El artículo 21, inc.3 del Anexo al Decreto Reglamentario Nº 182/2019 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

d) El artículo 21, inc.14 del Anexo al, Decreto Reglamentario Nº 182/2019 relativo a la protección de datos personales.

e) El artículo 1 de la, Resolución (ex) SMA N° 116-E/201 7, relativo a la captura de la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital.

Adicionalmente, el certificador celebra UN (1) acuerdo con el solicitante o suscriptor, conforme el Anexo V de la Resolución 946/2021 de la SECRETARÍA DE INNOVACIÓN PÚBLICA perteneciente a la JEFATURA DE GABINETE DE MINISTROS, del que surge su conformidad respecto a la veracidad de la información incluida en el certificado.

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

3.2.4 Información no verificada del suscriptor.

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

3.2.5 Validación de autoridad.

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

3.2.6 Criterios para la interoperabilidad.

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

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

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

La renovación sin presencia física
del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y las contraseñas necesarias para el acceso a su clave privada (PIN/OTP)" por lo que deberán detallar que la excepción a la presencia física es por única
•
vez.

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

a) después de la revocación de UN (1) certificado.

b) después de la expiración de UN (1) certificado.

c) antes de la expiración de UN (1) certificado.

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 humanas.

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.

La renovación sin presencia física del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y las contraseñas necesarias para el acceso a su clave privada.

7

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

La renovación sin presencia física del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y las contraseñas necesarias para el acceso a su clave privada.

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

3.4 Requerimiento de revocación.

La revocación podrá ser iniciada por el Suscriptor, por la Autoridad de Registro o por la AC.

Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del Certificador desde: http://www.encodeac.com.ar/firma-digital/revocacion.html

Este sitio se encuentra disponible las VEINTICUATRO (24) horas los SIETE (7) días de la semana, durante todo el año, lo que permite servicios de revocación en horarios no habituales de jornada laboral, como así también fines de semana y feriados. La solicitud de revocación se procesa automáticamente, de acuerdo a lo establecido en el punto "4.9.4- Plazo para la solicitud de revocación".

El Suscriptor que inicia la revocación se debe identificar en el portal con su clave de organización y luego con su PIN de revocación, obtenido durante el proceso de Solicitud, inicia el proceso de revocación de certificado.

En el caso de pérdida del PIN de revocación se deberá solicitar en el portal del Suscriptor el reenvío del mismo. Éste se enviará a la dirección informada por el Suscriptor, en forma automática.

7

La Autoridad de Registro o la AC de ENCODE S.A., podrán iniciar la revocación de certificados, según lo indicado en el inciso F del punto 4.9.2 del Anexo III de la Resolución N° 942/2021.

La Autoridad de Registro o la AC de ENCODE S.A., con la documentación relacionada a la causa de revocación, ingresan a la aplicación del Certificador con su usuario y clave, seleccionando el certificado a revocar que le pertenece al suscriptor e inicia el proceso automático de revocación que detecta el cambio de estado de la solicitud y lo incluye en la emisión de la siguiente lista de certificados revocados. Deja asentado en los registros informáticos de la AR la revocación efectuada.

En caso de presentarse personalmente ante la AR correspondiente, deberá contar con documento que permita acreditar su identidad y se registrarán los datos biométricos del solicitante de la revocación.

Para aquellos suscriptores, personas humanas o jurídicas, relacionados con una organización, ésta se obliga a:

1. notificar a la Autoridad de Registro de toda modificación de la situación del suscriptor que llevaría a inhabilitarlo como suscriptor de un certificado conforme a la presente Política Única de Certificación, o bien la modificación de los datos del suscriptor que llevarían a modificar la información contenida en el certificado expedido a favor de dicho suscriptor y
2. solicitar el requerimiento de revocación inmediata del certificado.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1 Solicitud de certificado.

4.1.1 Solicitantes de certificado.

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

4.1.2 Solicitud de certificado.

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

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2. Autenticación de la identidad de personas jurídicas públicas o privadas y 3.2.3. Autenticación de la identidad de personas humanas, así como la constancia de C.U.I.T. o C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores.

a) Solicitud de certificado de persona humana.

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el Solicitante, quien luego, debe acreditar fehacientemente su identidad según se indica en "3.2.3. Autenticación de la identidad de Personas Humanas".

Para poder efectuar la Solicitud de un certificado, el Solicitante debe:

- Contar con la clave de su organización para acceder a la aplicación del Certificador. El Solicitante deberá darse de alta en el sistema de su organización y registrarse. Si ya se encontrase registrado deberá ingresar su clave y contraseña en el sitio de su organización y seleccionar la pestaña "Solicitud de certificado" para ingresar al portal del Suscriptor.
- Contar con su dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado.
- Cumplir con los requisitos mínimos de configuración de hardware y software detallados en la "Guía del Solicitante" que se encuentra en: http://www.encodeac.com.ar/firma-digital/
- En caso de contar el Solicitante con un dispositivo criptográfico propio, de los modelos validados por el Certificador, deberá conectarlo previo al inicio de la sesión.

7

- En caso de utilizar un servicio de firma digital con custodia centralizada de claves criptográficas, éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.
- La aplicación, mostrará el formulario de Solicitud de persona humana con los datos históricos que tuviere almacenados del Solicitante, en caso de que alguno de los datos estuviera desactualizado, hubiera cambiado o fuera incorrecto, deberá ser modificado por el Solicitante en este mismo formulario. Completados los datos de la Solicitud, el Solicitante deberá confirmarlos.
- El Solicitante procederá a elegir libremente para realizar su identificación, seleccionando entre la Autoridad de Registro Central o una de las Autoridades de Registro Delegadas de ENCODE S.A.
- Habiendo confirmado los datos de la solicitud y elegido donde realizar la identificación, como medida de seguridad, se envía la solicitud al correo electrónico del titular declarado en la misma, solicitando la confirmación.
- Al ser confirmada la recepción del correo electrónico, la aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generará el par de claves criptográficas asimétricas.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. Si el Solicitante posee un dispositivo criptográfico podrá realizar la generación en el mismo. En caso contrario, la generación se hará por software.
- Generadas las claves, la aplicación del Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.
- El correo incluye: la Solicitud con el resumen criptográfico, los datos de la Autoridad de Registro con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, en los casos que corresponda se le informará importe y formas de pago disponibles.

b) Solicitud de certificado de persona jurídica.

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el responsable autorizado de la persona jurídica Solicitante, quien luego deberá acreditar fehacientemente su identidad según se indica en "3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas".

Para poder efectuar la solicitud de un certificado, el Solicitante debe:

- Estar registrado en el sistema de su organización. Deberá ingresar con su clave y su contraseña, y seleccionar la opción "Solicitud de Certificado" para ingresar a la aplicación del Certificador.
- Contar con su dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado
- Cumplir con los requisitos mínimos de configuración de hardware y software detallados en la "Guía del Solicitante" que se encuentra en: http://www.encodeac.com.ar/firma-digital/
- El proceso de solicitud podrá ser iniciado solamente por el responsable autorizado de la persona jurídica a favor de la cual se emitirá el certificado.
- La aplicación del Certificador verifica que la estación de trabajo del Solicitante cumple con los requerimientos técnicos mínimos. En caso de no cumplimentar los requerimientos técnicos mínimos el sistema le indicará las actualizaciones necesarias para solucionar dichos inconvenientes técnicos y de persistir los mismos deberá dirigirse a la Autoridad de Registro donde se le proporcionará un equipo preparado para que pueda realizar desde el mismo la suscripción utilizando un dispositivo criptográfico (hardware) propio para generación y el almacenamiento de su par de claves, y en ningún caso existirá contacto de la AR o AC de ENCODE S.A. con la clave privada del solicitante.
- En caso de contar el Solicitante con un dispositivo criptográfico (hardware) propio, deberá conectarlo previo al inicio de la sesión.
- En caso de utilizar un servicio de firma digital con custodia centralizada de claves criptográficas, éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.

- La aplicación le presenta la pantalla con el formulario de Solicitud de certificado de Persona Jurídica. La aplicación le traerá los datos históricos que tuviere almacenados la organización vinculada, en relación a la persona jurídica a favor de la cual se emitirá el certificado requerido, debiendo el solicitante proceder a su confirmación. En caso de que alguno de los datos registrados en la organización estuviera desactualizado, hubiera cambiado o fuera incorrecto, deberá ser modificado por el solicitante en este mismo formulario luego de lo cual confirmará los mismos.

- A continuación, le solicita todos los datos del Solicitante en su calidad de responsable autorizado de la persona jurídica.
- Completada la Solicitud, el Solicitante deberá confirmar todos los datos presentes en la misma.
- El Solicitante procederá a elegir libremente para realizar su identificación, seleccionando entre la Autoridad de Registro Central o una de las Autoridades de Registro Delegadas de ENCODE S.A.
- Habiendo confirmado los datos de la Solicitud y elegido el lugar para la identificación, como medida de seguridad, se la envía al correo electrónico declarado en la solicitud, solicitando la confirmación.
- Al ser confirmada la recepción del correo electrónico la aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generará el par de claves criptográficas asimétricas.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. Si el Solicitante posee un dispositivo criptográfico podrá realizar la generación en el mismo. En caso contrario la generación se hará por software.
- Generadas las claves, la aplicación del Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.
- El correo incluye: la Solicitud con el resumen criptográfico, los datos de la ubicación de la identificación con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, se le informará importe y formas de pago disponibles.

c) Solicitud de certificados de sitio seguro o de aplicación.

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el responsable autorizado de la persona jurídica solicitante, quien luego deberá acreditar fehacientemente su identidad según se indica en "3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas".

Para poder efectuar la solicitud de un certificado, el Solicitante DEBE:

- Completar el Formulario de Solicitud del certificado a través del portal de suscriptores y selecciona la opción de "Certificados SSL" para sitio seguro o "Certificados de aplicaciones" para aplicación.
- Contar con una dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado.
- Cumplir con los requisitos mínimos de configuración de hardware y software detallados en la "Guía del Solicitante" que se encuentra en: http://www.encodeac.com.ar/firma-digital/
- El proceso de solicitud podrá ser iniciado solamente por el responsable autorizado de la persona jurídica, titular del sitio seguro o aplicación a favor de la cual se emitirá el certificado.
- La aplicación del Certificador Licenciado verifica que la estación de trabajo del solicitante cumple con los requerimientos técnicos mínimos. En caso de no cumplimentar los requerimientos técnicos mínimos el sistema le indicará las actualizaciones necesarias para solucionar dichos inconvenientes técnicos y de persistir los mismos deberá dirigirse a la Autoridad de Registro donde se le proporcionará un equipo preparado para que pueda realizar desde el mismo la suscripción utilizando un dispositivo criptográfico propio para generación y el almacenamiento de su par de claves, y en ningún caso existirá contacto de la AR o AC de ENCODE S.A. con la clave privada del solicitante.
- La aplicación le presenta la pantalla con el formulario de Solicitud de Certificado. A continuación, le solicita todos los datos del Solicitante en su calidad de responsable autorizado de la persona jurídica.
- Completada la Solicitud, el Solicitante deberá confirmar todos los datos presentes en la misma.

7

- El Solicitante procederá a elegir libremente para realizar su identificación, seleccionando entre la Autoridad de Registro Central o una de las Autoridades de Registro Delegadas de ENCODE S.A.
- Habiendo confirmado los datos de la Solicitud y elegido el lugar para la identificación, como medida de seguridad, se le envía al correo electrónico declarado en la solicitud, solicitando la confirmación.
- Al ser confirmada la recepción del correo electrónico la aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generará el par de claves criptográficas asimétricas.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. Si el Solicitante posee un dispositivo criptográfico podrá realizar la generación en el mismo. En caso contrario la generación se hará por software.
- Generadas las claves, la aplicación del Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.
- El correo incluye: la Solicitud con el resumen criptográfico, los datos de la ubicación de la identificación con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, se le informará importe y formas de pago disponibles.

4.2 Procesamiento de la solicitud del certificado

Se describen a continuación las condiciones y procedimientos utilizados por el certificador para aceptar o rechazar la solicitud de un certificado.

Se indicará los plazos aplicables para la aceptación o rechazo de una solicitud, así como toda la información relativa a la tramitación de su certificado, de acuerdo al inciso h) del artículo 21 de la Ley N° 25.506 y en cumplimiento a lo establecido en la Resolución (ex) SMA N° 116-E/2017.

a) Solicitud de certificado de persona humana

- Cumpliendo el Solicitante con presentarse en la AR elegida, la aprobación de la Solicitud de certificado digital estará sujeta a cubrir los requerimientos para la verificación de la identidad del Solicitante y los requisitos específicos en relación con las características del certificado digital solicitado.
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.
- En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.
- Finalmente, en caso de aprobación de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.
- El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona humana Solicitante. Esta contiene la Solicitud de Certificado, los duplicados de todos los documentos presentados en un todo de acuerdo con lo especificado en la "Guía del Solicitante" y el "Acuerdo con Suscriptores" firmado.

a) Solicitud de certificado de persona jurídica

- La aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de los requerimientos para la verificación de la identidad del Solicitante y al cumplimiento de los requisitos específicos en relación a las características del certificado digital solicitado.
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.
- En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.
- Finalmente, en caso de aprobación de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

7

- El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona jurídica Solicitante. Esta contiene la Solicitud de Certificado, los duplicados de todos los documentos presentados y el "Acuerdo con Suscriptores" firmado.

b) Solicitud de certificados de sitio seguro o de aplicación

- En primer lugar, solamente para certificados de sitio seguro, se comprobará la documentación mediante consulta al registro de dominio correspondiente, verificará que el dominio está registrado.
- La aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de los requerimientos para la verificación de la identidad del Solicitante y al cumplimiento de los requisitos específicos en relación a las características del certificado digital solicitado.
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.
- En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.
- Finalmente, en caso de aprobación de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.
- El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona jurídica Solicitante. Esta contiene la Solicitud de Certificado, los duplicados de todos los documentos presentados y el "Acuerdo con Suscriptores" firmado.

4.3 Emisión del certificado

4.3.1 Proceso de emisión del certificado

Cumplidos los recaudos del proceso de identificación y autenticación de acuerdo con esta Política, y una vez aprobada la Solicitud por la Autoridad de Registro, la Autoridad

Certificante ENCODE S.A emite el correspondiente certificado, firmándolo digitalmente con su clave privada.

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

4.3.2 Notificación de emisión

El sistema pone el certificado en el Portal del Suscriptor, a disposición de su titular y le comunica esa disponibilidad por correo electrónico. El Portal del Suscriptor se encuentra en:

- **http://www.encodesa.com.ar/firma-digital/portal-suscriptor.html**

En este sitio web cada Solicitante puede acceder únicamente a su propia información.

4.4 Aceptación del certificado

Una vez notificado de la emisión de un certificado a su nombre, el Suscriptor o bien su responsable autorizado en caso de tratarse de certificados de personas jurídicas, de sitio seguro y de aplicaciones, deberá controlar su contenido y descargar el certificado desde el Portal del Suscriptor.

En caso de que existiera algún error u omisión en los datos del suscriptor contenidos en el certificado, deberá revocarlo con su PIN de revocación desde el Portal del Suscriptor, como se indica en "4.9.3.- Procedimientos para la solicitud de revocación".

En caso de formular un reclamo de no aceptación del certificado antes de descargar el mismo deberá realizarlo dentro de las 48 horas de la notificación de ENCODE S.A. de la puesta a disposición en el portal del suscriptor del certificado a su nombre. Ante la ausencia de reclamos a la Autoridad de Registro por parte del Suscriptor, en cuanto a los datos del certificado, se acepta la exactitud del contenido del certificado desde el momento de su notificación y el Suscriptor asume la totalidad de 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 Nº 25.506, en su artículo 25, el suscriptor debe:

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

b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;

c) Solicitar la revocación de su certificado al certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

Asimismo, se indicará que el suscriptor debe cumplir con las siguientes obligaciones:

a) Resguardar y no divulgar aquellos factores de autenticación (contraseñas de usuario, OTP, PIN) que permitan utilizar la clave privada.

b) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.

c) Utilizar los certificados de acuerdo a lo establecido en la Política de Única Certificación.

d) 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.

7

4.5.2 Uso de la clave pública y del certificado por parte 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 para 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 para de claves

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

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

La renovación sin presencia física del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y las contraseñas necesarias para el acceso a su clave privada.

Para los certificados de aplicaciones, incluyendo los de servidores, los responsables deben tramitar UN (1) nuevo certificado en todos los casos, cumpliendo los casos 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 Nº 25.506.

4.9.1 Causas de revocación

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

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de persona jurídica o aplicación
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial o Acto Administrativo de Autoridad competente.
- Por Resolución de la Autoridad de Aplicación.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.

- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
- Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario Nº 182/2019 y demás normativa sobre firma digital.
- Por revocación del certificado digital del Certificador.

La Autoridad Certificante de ENCODE S.A., 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 Licenciado o la Autoridad de Registro operativamente vinculada.

g) El Ente Licenciante.

7

h) La autoridad judicial competente.

i) La Autoridad de Aplicación.

4.9.3 Procedimientos para la solicitud de revocación

El certificador garantiza que:

a) Se identifica debidamente al solicitante de la revocación según se establece en el apartado 3.4.

b) Las solicitudes de revocación, así como toda acción efectuada por el certificador o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.

c) Se documentan y archivan las justificaciones de las revocaciones aprobadas.

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

e) El suscriptor del certificado revocado es informado del cambio de estado de su certificado.

Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del Certificador desde:

- **http://www.encodesa.com.ar/firma-digital/revocacion.html**

Este sitio se encuentra disponible las VEINTICUATRO (24) horas los SIETE (7) días de la semana, durante todo el año, lo que permite servicios de revocación en horarios no habituales de jornada laboral, como así también fines de semana y feriados.

Los suscriptores o sus responsables autorizados serán notificados en sus respectivas direcciones de correo electrónico del cumplimiento del proceso de revocación.

La revocación se reflejará en la próxima Lista de Certificados Revocados, cuando sea generada de acuerdo con lo especificado en el punto "4.9.7.- Frecuencia de emisión de lista de certificados revocados".

4.9.4 Plazo para la solicitud de revocación

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

El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas cumpliendo con lo establecido en el artículo 21, inc, 8 del Anexo al Decreto Reglamentario Nº 182/2019.

4.9.5 Plazo para el procesamiento de la solicitud de revocación

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

4.9.6 Requisitos para la verificación de la lista de certificados revocados

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

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

El certificador cumple con lo establecido en el artículo 21 inc.9 del Anexo al Decreto Reglamentario Nº 182/2019 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la Resolución N°946/2021 y sus correspondientes Anexos.

4.9.7 Frecuencia de emisión de listas de certificados revocados

La AC de ENCODE S.A. genera y publica periódicamente una única lista conteniendo todos los certificados revocados por ella, en forma acumulativa, en formato del CRL X.509 v2, sin superar las VEINTICUATRO (24) horas entre publicaciones.

4.9.8 Vigencia de la lista de certificados revocados

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

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

El certificador pone a disposición de los interesados la posibilidad de verificar el estado de un certificado por medio del acceso a la lista de certificados revocados y mediante el servicio de consultas en línea sobre el estado de los certificados (OCSP).

El certificador pone a disposición de los terceros usuarios:

a) La lista de certificados revocados en http://pki.encodesa.com.ar/firma-digital/crl/encode.crl y en http://pki2.encodesa.com.ar/firma-digital/crl/encode.crl

b) El servicio OSCP, accesible a través del sitio web http://ocsp.encodesa.com.ar/

c) Ambos servicios se encuentran disponibles SIETE por VEINTICUATRO (7x24) horas.

La verificación del estado de los certificados se puede realizar a través de las Listas de Certificados Revocados y el servicio OCSP.

7

4.9.10 Requisitos para la verificación en línea del estado de revocación

Se utiliza el protocolo OCSP que permite, mediante su consulta, determinar el estado de un certificado digital y es una alternativa al servicio de CRLs, el que también estará disponible. Este servicio es accedido a través del sitio web http://ocsp.encodesa.com.ar/. La respuesta de la consulta estará firmada con la clave del certificado OCSP correspondiente.

4.9.11 Otras formas disponibles para la divulgación de la revocación.

La Autoridad Certificante de ENCODE S.A. permite buscar un certificado y consultar su estado a ese instante desde el portal de suscriptores en: https://pki.encodesa.com.ar/consultarEstados.aspx

Para consumir este servicio el tercero usuario deberá poseer una computadora con conexión a Internet y un navegador web a fin de poder acceder al portal de suscriptores de ENCODE S.A.

4.9.12 Requisitos específicos para casos de compromiso de claves

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

4.9.13 Causas de suspensión

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

4.9.14 Autorizados a solicitar la suspensión

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

7

4.9.15 Procedimientos para la solicitud de suspensión

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

4.9.16 Límites del periodo de suspensión de un certificado

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

4.10 Estado del certificado

4.10.1 Características técnicas

Los servicios disponibles para la verificación del estado de los certificados emitidos por el Certificador son:

- Lista de certificados revocados (CRL).
- Servicio OCSP.

La CRL de la AC de ENCODE S.A, se emite cada UNA (1) hora con una vigencia de VEINTICUATRO (24) hs. Con respecto a OCSP, permite verificar si el certificado se encuentra vigente o ha sido revocado.

4.10.2 Disponibilidad del servicio

Los sistemas de distribución de CRLs y de consulta en línea del estado de los certificados estarán disponibles con un mínimo de NOVENTA Y NUEVE POR CIENTO (99%) anual y un tiempo programado de inactividad máximo de CERO COMA CINCO POR CIENTO (0.5%) anual.

4.10.3 Aspectos operativos

No aplicable.

4.11 Desvinculación del suscriptor

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

De igual forma se producirá la desvinculación, ante el cese de las operaciones del certificador.

4.12 Recuperación y custodia de claves privadas

En virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 25.506, la AC de ENCODE S.A. se obliga a no realizar bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados digitales. Asimismo, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley citada, el suscriptor de un certificado emitido en el marco de esta Política Única de Certificación se encuentra obligado a mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos e impedir su divulgación.

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 encuentra 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.

7

f) Medios de almacenamiento.

g) Disposición de material de descarte.

h) Instalaciones de seguridad externas.

5.2 Controles de Gestión

Se cuenta con controles de seguridad relativos a:

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, seguridad, limpieza, etcétera.

b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.

d) Frecuencia de procesos de actualización técnica.

e) Frecuencia de rotación de cargos.

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

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

7

5.4 Procedimientos de Auditoría de Seguridad

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

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

a) Tipo de eventos registrados. Se cumple lo establecido en el Anexo II Sección 3 Resolución N° 946/2021.

b) Frecuencia de procesamiento de registros.

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

d) Medidas de protección de los registros, incluyendo privilegios de acceso.

e) Procedimientos de resguardo de los registros.

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

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

h) Evaluación de vulnerabilidades.

5.5 Conservación de registros de eventos

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

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

Se respeta lo establecido en el Anexo II Sección 3 de la Resolución N° 946/2021 respecto del registro de eventos.

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

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

b) Período de guarda de los registros.

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

d) Procedimientos de resguardo de los registros.

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

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

g) Procedimientos para obtener y verificar la información archivada.

5.6 Cambio de claves criptográficas

El cambio del par de claves criptográficas de la Autoridad Certificante de ENCODE S.A., dará origen a la emisión de un nuevo certificado, por parte de la Autoridad Certificante Raíz de la República Argentina operada por la Autoridad de Aplicación.

La publicación de la nueva clave pública de la Autoridad Certificante de ENCODE S.A. se realiza en sus servidores, y se puede encontrar en el sitio web identificado como:

- **http://www.encodesa.com.ar/firma-digital**

Se mantiene el repositorio en línea accesible durante las VEINTICUATRO (24) horas, los SIETE (7) días de la semana.

Dos (2) años antes del vencimiento previsto del certificado de la Autoridad Certificante de ENCODE S.A. se solicitará la renovación de la licencia de la Política de Única de Certificación y el certificado correspondiente.

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 se encuentran desarrollados en el Plan de Contingencia.

Se han desarrollado procedimientos referidos a:

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

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

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

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

Los procedimientos cumplen con lo establecido por el artículo 20 del Anexo al Decreto Reglamentario Nº 182/2019 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8 Plan de Cese de Actividades

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

Se han implementado procedimientos referidos a:

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

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

c) Transferencia de la custodia de archivos y documentación e identificación de su custodio.

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

Se contempla lo establecido por el artículo 22 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el artículo 20 del Anexo del Decreto Reglamentario Nº 182/2019, reglamentario de la Ley de Firma Digital, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la Resolución N° 946/2021 y sus correspondientes Anexos.

6. CONTROLES DE SEGURIDAD TÉCNICA

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

6.1 Generación e instalación del par de claves criptográficas

La generación e instalación del par de claves es considerada desde la perspectiva de las autoridades certificantes del certificador, de los repositorios, del servicio de custodia centralizada de claves criptográficas, de las autoridades de registro y de los suscriptores.

6.1.1 Generación del par de claves criptográficas

La clave privada de la Autoridad Certificante de ENCODE S.A. es generada en ambientes seguros, por personal autorizado, sobre dispositivos criptográficos homologados FIPS 140-2 Nivel 3. Los propósitos para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización se encuentran descriptas en el "Acuerdo con Suscriptores".

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

La clave privada de los Oficiales de Registro es generada y almacenada por ellos, utilizando un dispositivo criptográfico validado por ENCODE S.A.

Los Oficiales de Registro generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

En el caso de los solicitantes y suscriptores, las claves son generadas y almacenadas por ellos mismos mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

- Las personas humanas podrán hacerlo a su elección por "software" o por "hardware" o a través de un "servicio de custodia centralizada de claves criptográficas"

En caso de elección por software las claves deben ser resguardadas con un PIN de seguridad para su acceso. Conforme al artículo 5 de la Resolución SIP N° 86/2020 no se permitirá la exportación de estos certificados con su correspondiente clave privada.

En el caso de elección por hardware, el dispositivo criptográfico deberá ser provisto por el suscriptor y debe estar dentro de los modelos especificados en la lista de los dispositivos validados por ENCODE S.A.

En caso de utilizar un "Servicio de custodia centralizada de claves criptográficas", éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.

- Las personas jurídicas podrán hacerlo a su elección por "software" o por "hardware" provisto por el suscriptor, sobre dispositivos criptográficos, validados por ENCODE S.A o por un Servicio de custodia centralizada de claves criptográficas. En este último caso el servicio deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.

Las claves de los suscriptores que cuenten con dispositivos criptográficos externos removibles deberán estar protegidas por tres factores de seguridad:

1. mediante la posesión del dispositivo por el suscriptor,
2. mediante una contraseña de acceso al dispositivo criptográfico definida por el propio suscriptor, mediante la contraseña de la clave privada definida por el propio suscriptor.

7

6.1.2 Entrega de la clave privada

Las claves privadas de los suscriptores y de los Oficiales de Registro son generadas por ellos mismos durante el proceso de Solicitud de Certificado, absteniéndose ENCODE S.A. de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firma.

6.1.3 Entrega de la clave pública al emisor del certificado

El Solicitante entrega la clave pública a la Autoridad Certificante de ENCODE S.A. durante el proceso de Solicitud de Certificado.

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

El Solicitante debe probar su identidad y demostrar que la solicitud le pertenece, presentándose a la Autoridad de Registro con la Solicitud en la cual se identifica el resumen criptográfico.

6.1.4 Disponibilidad de la clave pública del certificador

Los certificados de la Autoridad Certificante de ENCODE S.A., el certificado de la Autoridad Certificante Raíz de la República Argentina (ACR-RA) y el certificado digital OCSP se encuentran disponibles en un repositorio en línea de acceso público a través de Internet en la siguiente dirección:

- **http://www.encodesa.com.ar/firma-digital**

La verificación de la validez de los certificados de los suscriptores de la presente Política, se realiza automáticamente a través del siguiente procedimiento:

I) Verificando la cadena de confianza del certificado del suscriptor, que es una cadena de firmas y de certificados, que se realiza de la siguiente manera:

- Verificar el certificado con que se firma al certificado del suscriptor: Certificado de la Autoridad Certificante de ENCODE S.A., y
- Verificar el certificado con que se firma al certificado de la Autoridad Certificante de ENCODE S.A.: Certificado de la Autoridad Certificante Raíz de la República Argentina.

II) Verificando la vigencia y el estado de los certificados, a través de la consulta a las CRLs emitidas por la Autoridad Certificante de ENCODE S.A. y por la Autoridad Certificante Raíz.

6.1.5 Tamaño de claves

La Autoridad Certificante de ENCODE S.A. utiliza claves RSA con un tamaño de 4096 bits.

Los Oficiales de Registro utilizan claves RSA con un tamaño mínimo de 2048 bits.

Los suscriptores de certificados utilizan claves RSA con un tamaño mínimo de 2048 bits. El certificado digital de OCSP utiliza claves RSA con un tamaño mínimo de 4096 bits.

6.1.6 Generación de parámetros de claves asimétricas

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

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

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

`
7

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

La protección de la clave privada, considerada en este punto, se aplica para la Autoridad Certificante de ENCODE S.A., las Autoridades de Registro y los suscriptores.

6.2.1 Controles y estándares para dispositivos criptográficos

La clave privada de la Autoridad Certificante de ENCODE S.A. es generada y almacenada sobre un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 3.

Las claves privadas de los Oficiales de Registro son generadas y almacenadas sobre un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 2.

La clave privada del suscriptor persona humana es generada y almacenada, a elección del Solicitante,

1. por "software",
2. por "hardware" sobre dispositivos criptográficos de propiedad del suscriptor; el modelo del dispositivo debe ser alguno de los especificados en la lista de dispositivos validados por ENCODE S.A.
3. "Servicio de custodia centralizada de claves criptográficas" , que deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado

La clave privada del suscriptor persona jurídica, sitio seguro y aplicación es generada y almacenada, a elección del Solicitante,

1. por "software",
2. por "hardware" sobre dispositivos criptográficos de propiedad del suscriptor que cumplen con las normas FIPS 140-2 nivel 2. El modelo del dispositivo debe ser alguno de los especificados en la lista de dispositivos validados por ENCODE S.A.
3. "Servicio de custodia centralizada de claves criptográficas", que deberá estar integrado con los servicios de la Autoridad Certificante del Certificador

Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.

6.2.2 Control "M de N" de clave privada

La clave privada de la Autoridad Certificante es activada exclusivamente en las instalaciones de ENCODE S.A. o en su sitio alternativo de contingencia, dentro del nivel de seguridad asignado a las operaciones críticas de la Autoridad Certificante de ENCODE S.A.. Para su activación deben estar presentes, personal autorizado en un número M (3), de N (10) posibles.

Los Oficiales de Registro y los suscriptores de certificados con dispositivos criptográficos propios tienen acceso a su clave privada personal a través de una contraseña de acceso al dispositivo criptográfico y la contraseña de la clave privada.

6.2.3 Recuperación de clave privada

En caso de necesidad, la Autoridad Certificante de ENCODE S.A. prevé mecanismos de recuperación de su clave privada a partir de las copias de respaldo. Esta recuperación sólo puede ser realizada por personal autorizado, sobre dispositivos criptográficos seguros de los que dispone ENCODE S.A. y exclusivamente en los niveles de seguridad de la Autoridad Certificante de ENCODE S.A. en su sitio principal o en su sitio alternativo de contingencia.

No se implementan mecanismos de resguardo y recuperación de la clave privada de los Oficiales de Registro, ni de los suscriptores. En caso de compromiso de la clave privada, éstos deberán proceder a la revocación del certificado y tramitación de una nueva solicitud de emisión de certificado si así correspondiere.

6.2.4 Copia de seguridad de clave privada

Copias de la clave privada de la Autoridad Certificante de ENCODE S.A. son realizadas inmediatamente después de su generación, por personal autorizado de ENCODE S.A. y almacenadas en dispositivos criptográficos seguros validados FIPS 140-2 nivel 3. Estos dispositivos son resguardados en un lugar de acceso restringido.

No se implementan mecanismos de copias de resguardo de la clave privada de los Oficiales de Registro ni de los suscriptores.

6.2.5 Archivo de clave privada

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

6.2.6 Transferencia de claves privadas en dispositivos criptográficos

Las copias de resguardo de la clave privada de la Autoridad Certificante de ENCODE S.A. están soportadas en dispositivos criptográficos validados FIPS 140- 2 nivel 3.

6.2.7 Almacenamiento de claves privadas en dispositivos criptográficos

Las claves privadas de las Autoridades de Registro son generadas y almacenadas en dispositivos criptográficos validados FIPS 140-2 nivel 2 y no permiten su exportación.

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

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

6.2.8 Método de activación de claves privadas

Para la activación de la clave privada de la Autoridad Certificante de ENCODE S.A. se aplica el control M de N. Todos los responsables necesarios para la activación deberán

identificarse frente al sistema según corresponda al rol asignado y en un orden determinado por medio de distintos mecanismos de autenticación, a saber: llave de seguridad, claves secretas o ambos.

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

6.2.9 Método de desactivación de claves privadas

La desactivación de la clave privada de la Autoridad Certificante de ENCODE S.A. puede realizarse desactivando la partición que la contiene. Esta tarea requiere seguir un procedimiento de excepción, el que será debidamente autorizado por el Responsable de Firma Digital, quien, además, participará en la Ceremonia de desactivación de la clave privada de la Autoridad Certificante de ENCODE S.A..

6.2.10 Método de destrucción de claves privadas

Una vez finalizada la vida útil de la clave privada de la Autoridad Certificante de ENCODE S.A., la partición del dispositivo criptográfico contenedor de esa clave privada será borrada e inicializada a cero. Esta tarea se realizará en el Sitio de Máxima Seguridad en una Ceremonia preparada a ese efecto, con personal autorizado y con los procedimientos de seguridad establecidos.

Para el caso de que finalice la vida útil de la clave privada de un Oficial de una Autoridad de Registro o de un suscriptor, por motivo de revocación o expiración del certificado asociado, y sin mediar renovación, deberá eliminarse el certificado y su correspondiente clave privada.

6.2.11 Requisitos de los dispositivos criptográficos

La capacidad del módulo criptográfico de la Autoridad Certificante es expresada en cumplimiento como mínimo del estándar FIPS 140-2 nivel 3.

La capacidad del módulo criptográfico de los suscriptores y Oficiales de Registro es expresada en cumplimiento como mínimo del estándar FIPS 140-2 nivel 2.

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

6.3 Otros aspectos de administración de claves

6.3.1 Archivo permanente de la clave pública

Los certificados emitidos a Suscriptores y a los Oficiales de Registro, como así también el de la Autoridad Certificante de ENCODE S.A., son almacenados y publicados bajo un esquema de redundancia y respaldados en forma periódica.

Todos los certificados son almacenados en soporte magnético, en formato estándar bajo codificación internacional DER. Las políticas y controles de seguridad implementados para recuperar la clave pública archivada, incluyendo el software y hardware, se hallan descriptos en el "Plan de Contingencia".

6.3.2 Período de uso de clave pública y privada

Las claves privadas correspondientes a los certificados emitidos por el certificador podrán ser utilizadas por los suscriptores únicamente durante el período de validez de los certificados. Las correspondientes claves públicas podrán ser utilizadas durante el período establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su período de validez, según se establece en el apartado anterior.

6.4 Datos de activación

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

6.4.1 Generación e instalación de datos de activación

Los dispositivos criptográficos de hardware utilizados por los Oficiales de Registro y los suscriptores son inicializados por sus titulares

Como paso previo a la generación de la clave privada, los Oficiales de Registro y los suscriptores deberán establecer una clave de seguridad de acceso sobre el dispositivo criptográfico denominado contraseña y al momento de la generación, la contraseña de la clave privada.

La contraseña de acceso del dispositivo criptográfico y la contraseña de la clave privada, son conocidas sólo por su titular, ya sea un Oficial de Registro o un suscriptor, con el propósito de proteger la clave privada e impedir el acceso por parte de terceros, incluida la Autoridad Certificante de ENCODE S.A.

La generación e instalación de los datos de activación de la clave privada de la Autoridad Certificante de ENCODE S.A. se realiza durante la Ceremonia Inicial con la participación de los N posibles testigos del control M TRES (3) de N DIEZ (10).

6.4.2 Protección de los datos de activación

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

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

Los datos de activación de la clave privada de la Autoridad Certificante de ENCODE S.A. están protegidos por mecanismos de seguridad implementados en el nivel SEIS (6) del Sitio de Máxima Seguridad.

6.4.3 Otros aspectos referidos a los datos de activación

Es responsabilidad de los Oficiales de Registro y de los Suscriptores, elegir contraseñas para sus claves privadas y contraseñas de acceso del dispositivo criptográfico que:

- Contengan como mínimo OCHO (8) símbolos, que incluyan letras mayúsculas, letras minúsculas y números; y
- No sean fácilmente deducibles por otros, evitando utilizar nombres, direcciones, números telefónicos y similares relacionados con el Suscriptor.

La contraseña de acceso del dispositivo criptográfico debe diferir de la contraseña de la clave privada.

6.5 Controles de seguridad informática

6.5.1 Requisitos Técnicos específicos

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

Dichos requisitos se vinculan con los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación.

b) Separación de funciones entre los roles afectados al proceso de certificación.

c) Identificación y autenticación de los roles afectados al proceso de certificación.

d) Utilización de criptografía para las sesiones de comunicación y bases de datos.

e) Archivo de datos históricos y de auditoría del certificador y usuarios.

f) Registro de eventos de seguridad.

g) Prueba de seguridad relativa a servicios de certificación.

h) Mecanismos confiables para identificación de roles afectados al proceso de certificación.

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

Estas funciones pueden ser provistas por el sistema operativo, o bien a través de una combinación del sistema operativo, software de certificación y controles físicos.

6.5.2 Requisitos de seguridad computacional

Los servidores que conforman la Autoridad Certificante de ENCODE S.A. se encuentran alojados en el "Sitio de Máxima Seguridad" o SMS construido con los estándares requeridos para este tipo de ambientes.

Las certificaciones del módulo criptográfico HSM son las siguientes:

- U/L 1950 & CSA C22.2 y en CSA C22.2
- FCC Part 15 – Clase B
- High Assurance HSM
- Common criteria EAL 4+
- FIPS 140-2 Nivel 3

Los dispositivos criptográficos utilizados por los ORs y por los suscriptores están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2 o superior.

Los dispositivos criptográficos utilizados por los proveedores de otros servicios en relación a la firma digital están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2 como mínimo.

6.6 Controles Técnicos del ciclo de vida de los sistemas

ENCODE S.A. mantiene el control de los equipos y de la documentación de la configuración del sistema, registrándose toda modificación o actualización a cualquiera de ellos.

El esquema de seguridad física del SMS de la Autoridad Certificante de ENCODE

S.A. previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones.

El control periódico de integridad del sistema de la Autoridad Certificante de ENCODE S.A., realizado por el servicio de monitoreo, advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

6.6.1 Controles de desarrollo de sistemas

Los sistemas informáticos son homologados por personal técnico al momento de su implementación, para asegurar que los programas que se ponen en producción respondan a las características de diseño declarados por el proveedor y oportunamente aceptados cuando fueron seleccionados.

ENCODE S. A. ha adoptado el modelo de la organización OWASP (Open Web Application Security Project), como su estándar para la seguridad de los sistemas, que aplica tanto en los desarrollos que realiza como en la homologación del software adquirido y en las adaptaciones y el mantenimiento de aplicaciones.

6.6.2 Controles de gestión de seguridad

Se documenta y controla la configuración del sistema, así como toda modificación o actualización, habiéndose implementado un método de detección de modificaciones no autorizadas.

6.6.3 6Controles de seguridad del ciclo de vida del software

No es aplicable.

6.7 Controles de seguridad de red

ENCODE S. A. posee un sistema de protección integral de sus activos informáticos. La red de la Autoridad Certificante de ENCODE S.A., está aislada de otras redes y se encuentra delimitada por diversos cortafuegos (“firewalls”) que proveen el filtrado de los paquetes de datos.

6.8 Certificación de fecha y hora

El servicio de emisión de sellos de tiempo de la Autoridad Certificante de ENCODE

S.A. está basado en la especificación de los estándares RCF 3161 – "Internet X. 509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities, ETSI TS 101 861, "Time stamping profile" y a su especificación equivalente RFC 3628 – "Requirements for time-stamping authorities"; y está sincronizado con la hora oficial de la República Argentina.

Los sellos de tiempo gozarán de plena validez probatoria respecto a la fecha y hora de un documento digital firmado digitalmente, o de cualquiera de las instancias de su ciclo de vida.

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

El servicios de emisión de sellos de competencia y/o atributo prestados por el Encode S.A, está basado en la especificación de los estándares RFC 5755 "An Internet Attribute Certificate Profile for Authorization", respetando el formato y perfil definido en el anexo IV de la Resolución 946/2021.

Podrán ser autoridad de competencia todas aquellas entidades que tengan aptitud de acreditar una competencia, rol, función y o relación laboral con el titular de un certificado de firma digital.

Las autoridades de sello de competencia se conformarán mediante la celebración de un convenio con el certificador licenciado y la emisión del certificado de Autoridad de sello de competencia, pudiendo utilizar un servicio de custodia provisto por un certificador licenciado o bien implementar su propia infraestructura cumpliendo con los requisitos de seguridad establecidos en la resolución 946/2021, y satisfaciendo las condiciones para la implementación tecnológica del servicio de emisión de Sellos de Competencia y la documentación exigida para su funcionamiento establecidas por la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS o quien en el futuro la reemplace, de conformidad con el Art 51 del Anexo I de la citada resolución.

Las claves criptográficas de las Autoridades de Sello de Competencia serán generadas y almacenadas en un dispositivo criptográfico que cumpla con certificación FIPS 140 (Versión 2) nivel 3 o superior.

7. PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

Todos los certificados emitidos bajo la Política Única de Certificación de ENCODE *S.A.*respetan la especificación ITU-T X.509 (ISO/IEC 9594-8) "Information Technology – The Directory: Public key and atribute certificate frameworks" adoptada como estándar tecnológico para la Infraestructura de Firma Digital de la República Argentina por la Resolución 946/2021.

7.1 Perfil del certificado

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

El formato de los certificados digitales emitidos bajo esta política cumple con los requerimientos de la Resolución 946/2021 y las especificaciones contenidas en RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile" y RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Bajo esta Política Única de Certificación se emitirán 4 tipos de certificados para:

a) Persona humana

b) Persona Jurídica

c) Aplicación

d) Autoridad de Sello de Competencia

Perfil del certificado para Persona humana

Campo	Valor	
Version	2	
serialNumber	Número de Serie del certificado	
Signature	<Algoritmo de Firma> 2.16.840.1.101.3.4.1 (SHA256-RSA)	
Issuer	<Nombre Distintivo del Emisor>	
commonName	2.5.4.3	Autoridad Certificante ENCODESIN para Personas Físicas y Jurídicas
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	<Validez (Desde, Hasta)>	
notBefore	<fecha, hora, minutos y segundos de emisión>	
notAfter	<fecha, hora, minutos y segundos de emisión + 2 años>	
Subject	<Nombre Distintivo del Suscriptor>	
commonName	2.5.4.3	<Nombres y Apellidos>
serialNumber	2.5.4.5	<Tipo de documento y Numero de Documento>
countryName	2.5.4.6	<Nacionalidad de la Persona humana >
subjectPublicKeyInfo	<Clave Pública del Suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	contentCommitment, digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly igual a 1
SubjectAlternativeName	2.5.29.17	En caso de incluir el correo electrónico de la persona humana, se indicará en este campo.
CRLDistributionPoints	2.5.29.31	CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.encodesa.com.ar/firma-digital/crl/encode.crl CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki2.encodesa.com.ar/firma- digital/crl/encode.crl

CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=<OID de política asignado por la Autoridad de Aplicación> [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma- digital/encode.pdf userNotice=< certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506>
ExtendedKeyUsage	2.5.29.37	1.3.6.1.5.5.7.3.2 - Autenticación del cliente 1.3.6.1.5.5.7.3.4 - Correo seguro
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado ENCODE S.A. Además, para indicar la dirección donde puede accederse al servicio de OCSP.
QCStatement	1.3.6.1.5.5.7.1.3	Puede contener uno de los siguientes OIDs: 2.16.32.1.10.1, cuando las claves sean generadas por software 2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1 2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2 2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

Perfil del certificado para Persona Jurídica

Campo	Valor	
Version	2	
serialNumber	Número de serie del certificado	
Signature	<algoritmo de firma> 2.16.840.1.101.3.4.1 (SHA256-RSA)	
Issuer	<Nombre distintivo del emisor>	
commonName	2.5.4.3	Autoridad Certificante ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A.
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.

7

stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	<Validez (desde, hasta)>	
notBefore	<fecha, hora, minutos y segundos de emisión>	
notAfter	<fecha, hora, minutos y segundos de emisión + 2 años>	
Subject	<Nombre distintivo del suscriptor>	
commonName	2.5.4.3	Denominacion de la Persona Juridica o Unidad Operativa reponsable del Servicio (Ej., Ger RRHH)
serialNumber	2.5.4.5	<Código de Identificación y Numero de Iidentificación> CUIT+ Número de CUIT o Id Pais + Identificador Tributario para Personas Jurídicas Extranjeras
organizationalUnitName	2.5.4.11	<Unidad Operativas Relacionadas con el Suscriptor> (Pueden incluirse varias instancias de este atributo)
countryName	2.5.4.6	<País de emsión del Certificado>
subjectPublicKeyInfo	<clave pública del suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	contentCommitment, digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly igual a 1
SubjectAlternativeName	<Persona humana titular a cargo de la custodia de la clave>	
commonName	2.5.4.3	<Nombres y Apellidos>
serialNumber	2.5.4.5	<Tipo de documento y Numero de Documento>
Title	2.5.4.12	<Cargo o título de la persona titular a cargo de la custodia de la clave>

CRLDistributionPoints	2.5.29.31	CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.encodesa.com.ar/firma-digital/crl/encode.crl CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki2.encodesa.com.ar/firma-digital/crl/encode.crl
CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=<OID de política asignado por la Autoridad de Aplicación> [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma-digital/encode.pdf userNotice=< certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506>
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado ENCODE S.A. Además, para indicar la dirección donde puede accederse al servicio de OCSP.
QCStatement	1.3.6.1.5.5.7.1.3	Puede contener uno de los siguientes OIDs: 2.16.32.1.10.1, cuando las claves sean generadas por software 2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1 2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2 2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

Perfil del certificado para Aplicación

Campo	Valor
Version	2
serialNumber	Número de serie del certificado

7

Signature	<algoritmo de firma> 12.16.840.1.101.3.4.1 (SHA256-RSA)	
Issuer	<Nombre distintivo del emisor>	
commonName	2.5.4.3	Autoridad Certificante ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A.
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	<Validez (desde, hasta)>	
notBefore	<fecha, hora, minutos y segundos de emisión>	
notAfter	<fecha, hora, minutos y segundos de emisión + 2 años>	
Subject	<Nombre distintivo del suscriptor>	
commonName	2.5.4.3	<Denominacion de la aplicación o el servicio o la Unidad Operativa responsble>
serialNumber	2.5.4.5	<Código de Identificación y Numero de Iidentificación> CUIT+ Número de CUIT
organizationalUnitName	2.5.4.11	<Unidad Operativas de las que depende la aplicación o el servicio> (Pueden incluirse varias instancias de este atributo)
organizationName	2.5.4.10	<Denominación de la Persona Jurídica responsable de la aplicación o el servicio>
countryName	2.5.4.6	<País de emsión del Certificado>
subjectPublicKeyInfo	<clave pública del suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	nonRepudiation, digitalSignature,
		keyEncipherment igual a 1
SubjectAlternativeName	<Denominación de la aplicación o servicio>	
otherName		<Denominación de la aplicación o servicio>

CRLDistributionPoints		CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.encodesa.com.ar/firma-digital/crl/encode.crl CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki2.encodesa.com.ar/firma-digital/crl/encode.crl
CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=<OID de política asignado por la Autoridad de Aplicación> [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma-digital/encode.pdf userNotice=< certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506>
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado ENCODE S.A. Además, para indicar la dirección donde puede accederse al servicio de OCSP.
QCStatement	1.3.6.1.5.5.7.1.3	Puede contener uno de los siguientes OIDs: 2.16.32.1.10.1, cuando las claves sean generadas por software 2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1 2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2 2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

Perfil del certificado para Autoridad de Sello de Competencia

Campo	Valor
Version	2
serialNumber	Número de serie del certificado
Signature	<algoritmo de firma> 12.16.840.1.101.3.4.1 (SHA256-RSA)
Issuer	<Nombre distintivo del emisor>

7

commonName	2.5.4.3	Autoridad Certificante ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A.
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	<Validez (desde, hasta)>	
notBefore	<fecha, hora, minutos y segundos de emisión>	
notAfter	<fecha, hora, minutos y segundos de emisión + 2 años>	
Subject	<Nombre distintivo del suscriptor>	
commonName	2.5.4.3	<Denominación de la autoridad de competencia>
serialNumber	2.5.4.5	<Código de Identificación y Numero de Identificación> CUIT+ Número de CUIT
organizationalUnitName	2.5.4.11	<Unidad Operativas de las que depende la aplicación o el servicio> (Pueden incluirse varias instancias de este atributo)
organizationName	2.5.4.10	<Denominación de la Persona Jurídica responsable de la autoridad de competencia>
countryName	2.5.4.6	<País de emisión del Certificado>
subjectPublicKeyInfo	<clave pública del suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	nonRepudiation, digitalSignature,
		keyEncipherment igual a 1
SubjectAlternativeName	<Denominación de la Autoridad de Competencia>	
dnsName		<DNS del sitio web>
CRLDistributionPoints		CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.encodesa.com.ar/firma-digital/crl/encode.crl CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki2.encodesa.com.ar/firma-digital/crl/encode.crl

CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=<OID de política asignado por la Autoridad de Aplicación> [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma-digital/encode.pdf userNotice=< certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506>
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado ENCODE S.A. Además, para indicar la dirección donde puede accederse al servicio de OCSP.
QCStatement	1.3.6.1.5.5.7.1.3	Debe contener el siguientes OID: 2.16.32.1.10.2.3

7.1.1 Número de versión

Todos los certificados emitidos corresponder al estándar X.509 y contienen el valor 2 correspondiente a la versión 3.

7.1.2 Extensiones

Key Usage

El "keyusage" indica el uso del certificado de acuerdo con el RFC 5280 "Internet

X.509 Public Key Infrastructure Certificate and CRL Profile". Es una EXTENSIÓN CRÍTICA.

Extensión Políticas de Certificación

En la extensión de "certificatepolicies" (Politicas de Certificacion) debe detallar el nombre del dominio de la CA y el directorio creado para el Repositorio de dicho documento. Es una EXTENSIÓN CRÍTICA.

Se incluye OID de la Política de Certificación. Ese OID es asignado por la Autoridad de Aplicación a solicitud del ente licenciante.

7

Nombre Alternativo Del Sujeto

La extensión "subjectAltName", es una EXTENSIÓN NO CRÍTICA. En los certificados de personas jurídicas públicas o privadas que no identifiquen a un servicio se incluyen los datos identificatorios de la persona humana a cargo de la custodia de la clave privada del mismo.

Adicionalmente, esta extensión "SubjectAlternativeName" permite asociar identidades adicionales al suscriptor de un certificado. Las opciones definidas incluyen una dirección del correo electrónico, un nombre DNS, una dirección IP y un identificador uniforme de recurso (URI).

Esta extensión debe utilizarse para consignar las direcciones de correo electrónico de los suscriptores en lugar del atributo "email" del campo "subject".

Restricciones Básicas (Basic Constraints)

La extensión "BasicConstraints" permite identificar si el suscriptor de un certificado es un certificador e indica la longitud máxima de las rutas de certificación válidas que el certificado incluye. Esta extensión está presente en todos los certificados.

Los certificados de certificador deben contener el atributo "ca" con valor TRUE es una EXTENSIÓN CRÍTICA.

Para los certificados de usuarios finales deben dos contienen los atributos "ca" con valor FALSE y PathLenConstraint=Null.

Uso de Claves Extendido (Extended Key Usage)

La extensión permite configurar los propósitos de la clave. La extensión NO ES CRÍTICA.

Certificados para servicios de certificación digital de fecha y hora deben incluir el valor "id-kp- timeStamping" (1.3.6.1.5.5.7.3.8).

Los Certificados en caso de ser utilizados para correo seguro, deben incluir el valor "id-kp-email-protection" (1.3.6.1.5.5. 7.3.4)

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

7.1.3 Identificadores de algoritmos

El campo "signature" contiene el identificador de objeto (OID) del algoritmo y, si fueran necesarios, los parámetros asociados usados por el certificador para firmar el certificado. Este identificador será de los definidos en el [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA.

7.1.4 Formatos de nombre

Los formatos de nombres cumplen con lo establecido en el punto "3.1.2. Necesidad de Nombres Distintivos" de la Política Única de Certificación de ENCODE S.A.

7.1.5 Restricciones de nombre

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con "3.1.4. Reglas para la interpretación de nombres" y "3.1.5. Unicidad de nombres" de la Política Única de Certificación de ENCODE S.A.

7.1.6 OID de la Política de Certificación

El OID de la Política de Certificación que AC de ENCODE S.A. utiliza para la emisión de sus certificados, fue asignado por la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS (s/ Art 15, Decreto 1063/2016, MINISTERIO DE MODERNIZACIÓN), a solicitud del ente licenciante.

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

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

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

7.1.7 Sintaxis y semántica de calificadores de Política

El calificador de la política está incluido en la extensión de "certificate policies" y contiene una referencia al URL con la Política de Certificación aplicable

7.1.8 Semántica de procesamiento para extensiones críticas

Sin estipulaciones.

7.2 Perfil de la lista de certificados revocados

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 el punto "3 - Perfil de CRLs" del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados de la Resolución N° 946/2021.

Campo	Valor	
Version	1	
Signature	<Algoritmo de Firma> 2.16.840.1.101.3.4.1 (SHA256-RSA)	
Issuer	<Nombre Distintivo del Emisor>	
commonName	2.5.4.3	Autoridad Certificante ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A.
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
thisUpdate	<fecha, hora, minutos y segundos de emisión>	
nextUpdate	<fecha, hora, minutos y segundos de próxima emisión>	
revokedCertificates	<Certificados Revocados>	
serialNumber	<serialNumber del certificado revocado>	
revocationDate	<fecha de revocación>	
ReasonCode	<motivo de revocación del certificado>	
Extensions	<Extensiones >	
IssuingDistributionPoint	2.5.29.28	<URL de punto de distribución>
InvalidityDate	2.5.29.24	Fecha en la que se invalidó el certificado

7

CertificateIssuer	2.5.29.2	Emisor del certificado asociado con una entrada en una CRL indirecta
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
CRLNumber	2.5.29.20	<Nro. de secuencia de CRL>

7.2.1 Número de versión

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

7.2.2 Extensiones de CRL (Lista de Certificados Revocados)

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

La extensión "AuthorityKeyIdentifier" proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL.

Esta extensión está presente en todas las listas de revocación de certificados.

Número de CRL (CRL Number)

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

Esta extensión se encuentra en todas las listas de revocación de certificados.

Punto de Distribución del Emisor (Issuing Distribution Point)

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

Perfil de la consulta en línea del estado del certificado

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

7

7.2.3 Consultas OCSP

Los siguientes datos se encuentran presentes en las consultas:

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

Al recibir la consulta OCSP, se determina:

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

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

7.2.4 Respuestas OCSP

Todas las respuestas OCSP son firmadas digitalmente por la Autoridad certificante de ENCODE S.A. y contienen los siguientes datos:

- Versión de la sintaxis de respuesta.
- Identificador de quien responde.
- Fecha y hora en la que se genera la respuesta.
- Respuesta respecto al estado del certificado.
- Extensiones opcionales.
- Identificador (OID) único del algoritmo de firma.
- Firma de la respuesta.

La respuesta a una consulta OCSP consiste en:

7

- Identificador del certificado.
- Valor correspondiente al estado del certificado.
- Período de validez de la respuesta.
- Extensiones opcionales.

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

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

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Encode SA, en su carácter de certificador licenciado, se encuentra sujeto a las auditorias dispuestas en artículo 34 de la Ley N° 25.506 y sus modificatorias.

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

Los temas principales a evaluar en dichas auditorías son:

- Requisitos legales generales.
- Política Única de Certificación y Manual de Procedimientos de Certificación.
- Plan de Seguridad.
- Plan de Cese de Actividades.
- Plan de Contingencia.
- Plataforma Tecnológica.
- Ciclo de vida de las claves criptográficas del certificador.
- Ciclo de vida de los certificados de suscriptores.
- Estructura y contenido de los certificados y CRLs.
- Mecanismos de acceso a la documentación publicada, certificados y CRLs.
- Guía de instalación y funcionamiento de las Autoridades de Registro.

Por su parte, ENCODE S.A. realizará auditorías periódicas a las Autoridades de Registro habilitadas, para verificar el cumplimiento de los requisitos de su habilitación, siendo los temas principales a evaluar:

- Lo establecido en el documento reservado "Guía de instalación y funcionamiento de las Autoridades de Registro", disponible en la Autoridad de Registro Central de Encode S.A.

- Las políticas y procedimientos aprobados por el Ente Licenciante para la presente Política Única de Certificación.

En caso de producirse observaciones en las auditorías realizadas, luego de haber sido debidamente notificadas a ENCODE S.A., ésta tomará las medidas correctivas de carácter legal y técnico que amerite el caso.

En cumplimiento del artículo 33 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría, el artículo 21, inciso k) de la misma Ley, relativo a la publicación de informes de auditoría, y el artículo 7 del Anexo al Decreto Nº 182 E/2019, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría; la información relevante de los informes de la última auditoría realizada por el Organismo Auditante, es publicada en los sitios mencionados en el apartado "2.2 - Publicación de información del certificador". Asimismo, ENCODE SA realizará auditorías periódicas sobre los procesos de la propia AC para verificar el permanente cumplimiento de los requisitos de su habilitación.

9. ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1 Aranceles

Los certificados digitales emitidos bajo la presente política son expedidos a favor de personas humanas, de personas jurídicas, sitios seguros y aplicaciones a título oneroso, aplicándose aranceles diferenciales asociados conforme al tipo de certificado:

Los aranceles serán publicados en el sitio web ENCODE S. A. al que se accede mediante:

- **http://www.encodesa.com.ar/firma-digital/aranceles.html**

El solicitante/suscriptor del certificado deberá pagar el arancel de su certificado. Con el comprobante para el pago emitido a ese efecto, podrá abonar en la Autoridad de Registro Central o en los medios de pago que se indican en la siguiente dirección:

- **http://www.encodesa.com.ar/firma-digital/medio de pago.html**

9.2 Responsabilidad Financiera

Las responsabilidades financieras se originan en la Ley Nº 25506 y lo establecido por ENCODE S.A. a los efectos de esta Política Única de Certificación. La parte pertinente de esa norma es transcripta a continuación.

"Obligaciones impuestas por la ley Nº 25.506, artículo 38

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, 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.

Los certificadores no son responsables en los supuestos del artículo 39 de la Ley N° 25.506."

9.3 Confidencialidad

Todos los datos correspondientes a las personas humanas y jurídicas a las cuales alcance esta Política Única de Certificación están sujetos a las estipulaciones de la Ley Nº 25.326 de Protección de los Datos Personales.

Como principio general, se establece que toda información remitida por el solicitante de un certificado al momento de efectuar un requerimiento debe ser considerada confidencial y no ser divulgada a terceros sin el consentimiento previo del solicitante o suscriptor, salvo que sea requerida por juez competente o bien como parte de un proceso judicial o administrativo. 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.

9.3.1 Información confidencial

La protección abarca a la siguiente información, en la medida en que no sea de conocimiento público:

- Toda la información remitida por el solicitante o suscriptor a la Autoridad de Registro, excepto los datos que figuran en el certificado.
- Cualquier información almacenada en servidores o bases de datos destinadas a firma digital.
- Cualquier información impresa o transmitida en forma verbal referida a procedimientos, manual de procedimientos, etc., salvo aquellos que en forma expresa fueran declarados como no confidenciales.
- Cualquier información referida a planes de contingencia, controles o procedimientos de seguridad, registros de auditoría creados y/o mantenidos por ENCODE S.A.

La presente lista es de carácter ilustrativo, resultando confidencial toda información del proceso de firma digital que expresamente no señale lo contrario. La regla general es que toda información que no sea considerada como pública revestirá el carácter de confidencial.

Durante el ciclo de vida del certificado, tanto ENCODE S.A. como sus Autoridades de Registro no podrán divulgar los datos de los suscriptores sin su consentimiento. Asimismo, ENCODE S.A. se compromete a hacer público exclusivamente los datos del suscriptor que resulten imprescindibles para el reconocimiento de su firma digital.

Se declaran expresamente como confidenciales:

- La clave privada de la Autoridad Certificante de ENCODE S.A. La Autoridad Certificante garantiza la confidencialidad frente a terceros de su clave privada, la cual, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifica en la presente política.

- Las claves privadas de los solicitantes y suscriptores. Para garantizar la confidencialidad de las claves de autenticación y firma de los solicitantes o suscriptores, ENCODE S.A. proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro. Las claves serán generadas por el propio solicitante y almacenadas en un equipo o dispositivo criptográfico de hardware. A su vez, ni las Autoridades de Registro ni la Autoridad Certificante de ENCODE S.A. tendrán la posibilidad de generar, almacenar, copiar o conservar información que permita reconstruir o activar las claves privadas de solicitantes y suscriptores.

9.3.2 Información no confidencial

La siguiente información no se considera confidencial:

a) Contenido de los certificados y de las listas de certificados revocados.

b) Información sobre personas humanas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público.

c) Políticas de Certificación y Manual de Procedimientos de Certificación

d) Secciones públicas de la Política de Seguridad del certificador.

e) Política de privacidad del certificador.

9.3.3 Responsabilidades de los roles involucrados

Los roles de ENCODE SA se hallan descriptos en el documento "Roles y Funciones", que define las principales funciones, responsabilidades, obligaciones y tareas, donde se detalla las responsabilidades pertinentes para aquellos que gestionan información confidencial, con el fin de evitar su compromiso o divulgación a personas no autorizadas.

9.4 Privacidad

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

7

9.5 Derechos de Propiedad Intelectual

ENCODE S. A. es propietaria exclusiva de todos los derechos de propiedad intelectual de la presente política, acuerdos, declaraciones, procedimientos y documentos auxiliares referidos a la Autoridad Certificante de ENCODE S.A., así como la documentación y contenidos del sitio web de la Autoridad Certificante de ENCODE S.A. que se encuentra en:

- **http://www.encodesa.com.ar/firma-digital**

Asimismo, es titular del derecho de propiedad intelectual de las aplicaciones informáticas propias, excepto los sistemas operativos de soporte informáticos no desarrollados por ENCODE SA que cuentan con sus respectivas licencias de uso.

ENCODE SA es única y exclusiva propietaria de la presente Política Única de Certificación, y sus documentos relacionados reservándose todos los derechos de autor establecidos en la legislación vigente de derechos de propiedad intelectual.

9.6 Responsabilidades y garantías

I) Responsabilidades

En un todo de acuerdo con la Ley Nº 25.506 de Firma Digital, Capítulo IX, existirán dos supuestos de responsabilidad civil

I.a) Responsabilidades del Certificador y el Suscriptor

Existen responsabilidades mutuas entre el certificador licenciado que emite un certificado y el titular de dicho certificado.

Sin perjuicio de las previsiones de la citada ley, y demás legislación vigente, la relación entre ENCODE S. A. y el titular de un certificado se regirá por el acuerdo que se celebre entre ellos, conforme al artículo 37 de la Ley N° 25.506. El modelo de acuerdo está identificado como Acuerdo con Suscriptores y se puede consultar, al igual que otra información disponible, en el sitio web de ENCODE S. A. identificado como:

- **http://www.encodesa.com.ar/firma-digital**

I.b) Responsabilidades del Certificador ante Terceros usuarios

7

El Certificador que emita un certificado digital, o lo reconozca en los términos del artículo 16 de la Ley N° 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.

II)Garantías

II.a) Garantías del Certificador Licenciado

Además de lo estipulado en la Política Única de Certificación, el Certificador Licenciado garantiza que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión de los mismos.
- No existan errores en la información que fue introducida por la entidad que aprueba la emisión del certificado.
- Los certificados reúnen los requerimientos expuestos en esta Política Única de Certificación.

II.b) Garantías de la Autoridad de Registro

Además de lo estipulado en la Política Única de Certificación, la Autoridad de Registro garantiza que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No se presentan errores en la información del certificado que fue presentada a la Autoridad de Registro.
- Los dispositivos y materiales requeridos cumplen con lo dispuesto en esta Política Única de Certificación.

II.c) Garantías del suscriptor

Además de lo estipulado en la Política Única de Certificación, el suscriptor garantiza que:

- Cada firma digital creada usando la clave privada corresponde a la clave pública listada en el certificado.
- La clave privada está protegida y que no autoriza a otras personas a tener acceso a la clave privada del suscriptor.
- Toda la información facilitada por el suscriptor y contenida en el certificado es verdadera.
- El certificado es utilizado exclusivamente para los propósitos autorizados.

II.d) Garantías de los Terceros Usuarios

- Los Terceros Usuarios deben garantizar que han solicitado conocer suficiente información para tomar la decisión de aceptar el certificado.

9.7 Deslinde de responsabilidad

ENCODE S.A en su carácter de Certificador Licenciado no es responsable en los 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;
- 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.

7

9.8 Limitaciones a la responsabilidad frente a terceros

I) Limitaciones de responsabilidad legal

ENCODE S.A. establece en su Política Única de Certificación, Manual de Procedimientos u otra documentación relevante cualquier limitación de responsabilidad que pudiera aplicársele, considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación establecidas en este documento.

II)Limitaciones de responsabilidad del Certificador Licenciado

Dentro de los límites permitidos por la normativa vigente que rige la materia, en el Acuerdo de Suscriptores se establece y limita la responsabilidad tanto de suscriptores como de la propia Autoridad Certificante de ENCODE S.A. Las limitaciones de responsabilidad incluyen una exclusión de daños indirectos, especiales, incidentales y derivados.

9.9 Compensaciones por daños y perjuicios

No es aplicable.

9.10 Condiciones de vigencia

I) Período de vigencia de la Política Única de Certificación

La Política Única de Certificación empieza a ser efectiva una vez publicada en su sitio de internet, previa aprobación de la Autoridad de Aplicación, y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la Política Única de Certificación.

II)Finalización

La Política Única de Certificación se encuentra vigente mientras no se derogue expresamente por la emisión de una nueva versión.

III) Finalización de la Política Única de Certificación, efectos y vigencia de los certificados

La finalización de la vigencia de la Política Única de Certificación puede ser por derogación expresa, enmiendas o modificaciones; todos los certificados emitidos bajo esa política seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Política Única de Certificación contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

9.11 Avisos personales y comunicaciones con los participantes

No es aplicable

9.12 Gestión del ciclo de vida del documento

La presente Política Única de Certificación contempla las siguientes fases de su ciclo de vida:

- Planificación – Se identifican y documentan las principales oportunidades de mejora o necesidades de cambio.
- Evaluación – Los posibles cambios se documentan en categorías características (por ej: técnicos, operativos, etc.) y cuantificarlos según una escala numérica conforme a su probabilidad e impacto.
- Aprobación – Si el cambio es aceptado de acuerdo a la evaluación previa, lo autoriza el Responsable de Firma Digital de ENCODE S.A. A continuación, todo cambio será sometido a la aprobación de la Autoridad de Aplicación y/o Ente Licenciante Modificación – Si el cambio es aprobado, se implementa en una nueva versión de la Política

    - Publicación – En el sitio web de ENCODE S.A.

    - Puesta en vigencia.

7

9.12.1 Procedimientos de cambio

Esta Política Única de Certificación y sus documentos complementarios serán revisados por ENCODE S.A. en forma periódica para detectar y corregir eventuales faltas de claridad y para adaptarlos a cambios en la normativa.

Todo cambio será sometido a la aprobación de la Autoridad de Aplicación y/o Ente Licenciante y, una vez aprobado, publicado en el sitio web de ENCODE S.A. y puesto en vigencia.

Cada nueva versión tendrá una descripción de los cambios producidos referidos a la versión previa.

9.12.2 Mecanismo y plazo de publicación y notificación

I) Procedimientos de publicación y notificación

Una copia actualizada del presente documento se encuentra permanentemente disponible en forma pública y accesible a través de Internet en la dirección:

- **http://www.encodesa.com.ar/firma-digital/encode.pdf**

En caso de producirse modificaciones sustanciales a los contenidos de la presente política, los suscriptores que posean certificados vigentes a la fecha de aplicación del cambio serán notificados por correo electrónico en las direcciones declaradas en los correspondientes certificados.

II)Procedimientos de aprobación

Según lo establecido por el Art. 21 inc. q) de la Ley 25.506 por Art. 45 de la Resolución N° 946/2021 y Art. 23 inc. 24 del Anexo al Decreto N°182 E/2019, la presente política y sus posteriores modificaciones deben ser aprobadas por la Autoridad de Aplicación y/o Ente Licenciante de Firma Digital de la República Argentina.

9.12.3 Condiciones de modificación del OID

No aplicable.

9.13 Procedimientos de resolución de conflictos

En caso de surgir cualquier discrepancia o conflicto interpretativo o de cualquier índole entre las partes, se deberá realizar un reclamo por escrito dirigido a

ENCODE S. A., en su condición de Certificador Licenciado.

ENCODE S. A. intentará resolverlos mediante el siguiente procedimiento administrativo a su cargo:

- Una vez recibida la descripción del conflicto y constatada la divergencia, labrará un acta que deje expresa constancia de los hechos que la motivan y de todos y cada uno de los antecedentes que le sirvan de causa.
- Dará traslado del acta, mediante notificación fehaciente, a las partes involucradas: Autoridad de Registro y/o Suscriptor y/o Tercero usuario. Estas partes dispondrán de un plazo de diez (10) días corridos para ofrecer y producir la prueba que haga a su defensa y aleguen sobre el mérito de la misma.
- Finalmente, ENCODE S. A. resolverá en un plazo de DIEZ (10) días corridos lo que estime corresponder, conforme a criterios de máxima razonabilidad, equidad y pleno ajuste a la normativa vigente y aplicable en la especie.
- Las partes involucradas en el conflicto podrán recurrir ante la Autoridad de Aplicación, previo agotamiento del procedimiento administrativo recién descripto y sin perjuicio de su derecho de acudir directamente a la vía judicial correspondiente.

Los registros electrónicos almacenados bajo condiciones de seguridad razonables y grabados sistemáticamente en un medio permanente e inalterable constituyen plena evidencia del cumplimiento de las obligaciones del certificador y de sus Autoridades de

7

Registros, como así también de las comunicaciones, contratos y pagos hechos entre las partes.

9.14 Legislación aplicable

La legislación que respalda la interpretación, aplicación y validez de la Política de Certificación, es la Ley N° 25.506 y su modificatoria, el Decreto Nº 182 E/2019 y su modificatoria y toda otra norma complementaria dictada por la autoridad competente.

9.15 Conformidad con normas aplicables

A los fines de la interpretación y aplicación de la presente Política Única de Certificación se debe tener en cuenta la normativa que la rige.

En caso de reclamos de los usuarios o suscriptores de certificados digitales relacionados con la prestación de servicios de ENCODE S. A., el suscriptor o tercero deberá realizar el correspondiente reclamo en forma fehaciente ante ENCODE S.A. y, en caso de haber resultado infructuoso, podrá efectuar una denuncia ante la Autoridad de Aplicación, sin perjuicio de dejar a salvo los derechos de las partes en conflicto de recurrir a la vía judicial cuando así lo creyeren conveniente.

9.16 Cláusulas adicionales

No es aplicable.

9.17 Otras cuestiones generales

No es aplicable.

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Anexo Disposición

Número: DI-2021-109964170-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Viernes 12 de Noviembre de 2021

Referencia: Política Única de Certificación - ENCODE S.A.

El documento fue importado por el sistema GEDO con un total de 99 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.11.12 13:55:51 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2021.11.12 13:55:52 -03:00