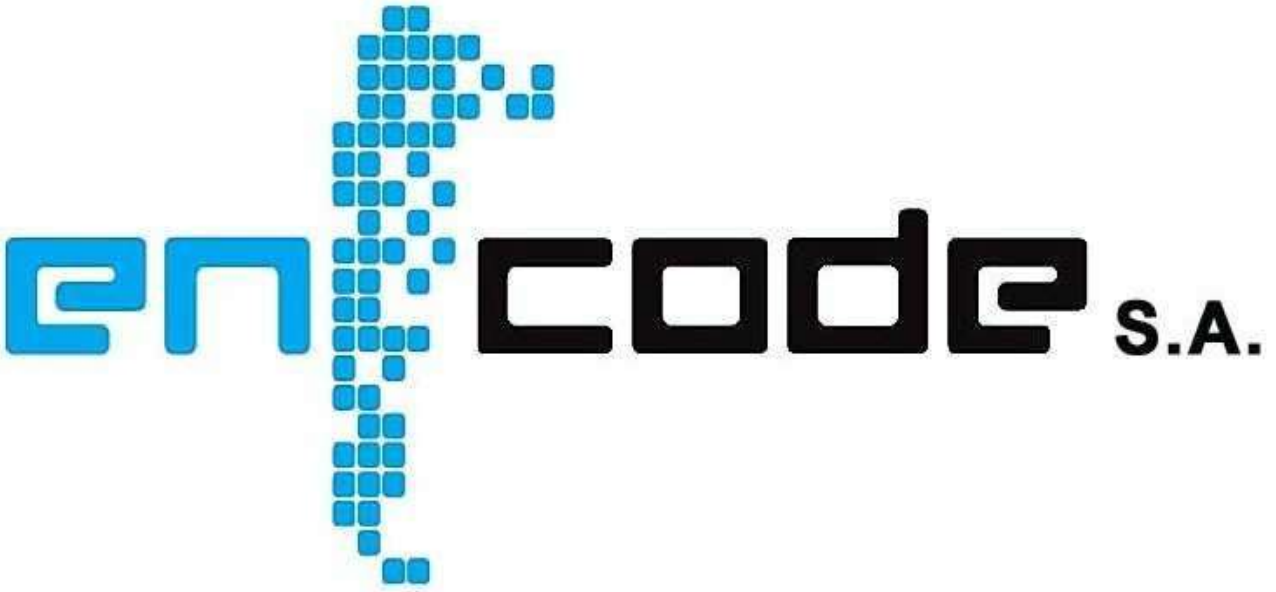

MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN (PÚBLICO)

POLÍTICA ÚNICA DE CERTIFICACIÓN DE ENCODE S.A

CLASE: PÚBLICO

Versiones y modificaciones de este documento.

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	2010-07-16	GrupoFD	Directorio ENCODE	Aprobación para presentación
1	1	2011-06-24	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	2	2011-08-18	GrupoFD	Directorio ENCODE	Clase Certificado, Puesto atención, Suscriptor, Aplicaciones Habilitadas, Período de uso, FIPS, OWASP
1	3	2011-09-26	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	4	2011-11-01	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	5	2011-11-23	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	6	2014-11-10	GrupoFD	Directorio ENCODE	Adecuación a Política Única
1	7	2014-11-20	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	8	2014-12-05	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	9	2020-11-11	GrupoFD	Directorio ENCODE	Adecuación Resolución 399 y Servicio de custodia
1	10	2020-12-29	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	11	2021-03-15	GrupoFD	Directorio ENCODE	Aprobación modificaciones

1. INTRODUCCIÓN.....6
1.1. Descripción general.....6
1.2. Nombre e Identificación del Documento.....6
1.3. Participantes.....6
1.4. Uso de los certificados.....7
1.5. Administración del Manual de Procedimientos.....7
1.6. Definiciones y Acrónimos.....8
2. RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS.....11
2.1. Repositorios.....11
2.2. Publicación de información del certificador.....11
2.3. Frecuencia de publicación.....11
2.4. Controles de acceso a la información.....11
3. IDENTIFICACIÓN Y AUTENTICACIÓN.....12
3.1. Asignación de nombres de suscriptores.....12
3.2. Registro inicial.....14
3.3. Identificación y autenticación para la generación de nuevo par de claves (Rutina de Re Key) 20
3.4. Requerimiento de revocación.....21
4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.....25
4.1. Solicitud de Certificado.....25
4.2. Procesamiento de la solicitud del certificado.....30
4.3. Emisión del certificado.....31
4.4. Aceptación del certificado.....33
4.5. Uso del par de claves y del certificado.....33
4.6. Renovación del certificado sin generación de un nuevo para de claves.....34
4.7. Renovación del certificado con generación de un nuevo para de claves.....34
4.8. Modificación del certificado.....34
4.9. Suspensión y Revocación de Certificados.....35
4.10. Estado del certificado.....40
4.11 Desvinculación del suscriptor.....40
4.12 Recuperación y custodia de claves privadas.....40
5. CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN.....41

5.1 Controles de seguridad física 41
5.2 Controles de Gestión 41
5.3 Controles de seguridad del personal 42
5.4 Procedimientos de Auditoría de Seguridad 49
5.5 Conservación de registros de eventos 50
5.6 Cambio de claves criptográficas 53
5.7 Plan de respuesta a incidentes y recuperación ante desastres 53
5.8 Plan de Cese de Actividades 54
6. CONTROLES DE SEGURIDAD TÉCNICA 56
6.1. Generación e instalación del par de claves criptográficas 56
6.2. Protección de la clave privada y controles sobre los dispositivos criptográficos 56
6.3. Otros aspectos de administración de claves 60
6.4. Datos de activación 60
6.5. Controles de seguridad informática 61
6.6. Controles Técnicos del ciclo de vida de los sistemas 63
6.7. Controles de seguridad de red 64
6.8. Certificación de fecha y hora 64
7. PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS 66
7.1. Perfil del certificado 65
7.2. Perfil de la lista de certificados revocados 65
7.3. Perfil de la de la consulta en línea del estado del certificado 65
8. AUDITORÍAS DE CUMPLIMIENTO Y OTRAS EVALUACIONES 67
9. ASPECTOS LEGALES Y ADMINISTRATIVOS 69
9.1. Aranceles 69
9.2. Responsabilidad Financiera 70
9.3. Confidencialidad 70
9.4. Privacidad 70
9.5. Derechos de Propiedad Intelectual 71
9.6. Responsabilidades y garantías 71
9.7. Deslinde de responsabilidad 71
9.8. Limitaciones a la responsabilidad frente a terceros 71

9.9. Compensaciones por daños y perjuicios 71
9.10. Condiciones de vigencia 71
9.11. Avisos personales y comunicaciones con los participantes 72
9.12. Gestión del ciclo de vida del documento 73
9.13. Procedimiento de resolución de conflictos 73
9.14. Legislación aplicable 75
9.15. Conformidad con normas aplicables 75
9.16. Clausulas adicionales 75
9.17. Otras cuestiones generales 75

1. INTRODUCCIÓN

1.1. Descripción general

El Manual de Procedimientos de Certificación describe las actividades requeridas para la puesta en marcha y prestación del servicio de certificación de ENCODE S.A. como Certificador Licenciado y está estrechamente ligado al documento Política Única de Certificación de ENCODE S.A.

Esas actividades constituyen procedimientos específicos, para cada uno de los cuales se indican todos o algunos de los siguientes datos:

- Consideraciones
- Requisitos
- Objetivo
- Frecuencia, oportunidad y urgencia
- Roles que participan en el procedimiento
- Acción que pone en marcha el procedimiento
- Tareas a realizar por cada uno de los roles que actúan
- Resultado del procedimiento

Este Manual está dividido en dos partes, presentadas como dos documentos por separado, pero con una estrecha relación, dado que uno es complementario del otro.

1.2. Nombre e Identificación del Documento

Nombre: Manual de Procedimientos de Certificación de ENCODE SA (Público)
Versión: 1.11
Fecha: 15/03/2021
Lugar: República Argentina

1.3. Participantes

1.3.1. Certificador

ENCODE S.A. en su calidad de Certificador Licenciado, con licencia otorgada por Resolución Nº 184/2012 de la ex Secretaría de Gabinete en su carácter de Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina (IFDRA), presta los servicios de certificación digital según lo establecido por la Ley N° 25.506 y sus normas complementarias.

A los fines de desarrollar las referidas tareas se constituye la Autoridad Certificante de

ENCODE S.A., en adelante “Autoridad Certificante” o “Autoridad Certificante ENCODE S.A”.

1.3.2. Autoridad de Registro

Las tareas relacionadas con la identificación y autenticación de los solicitantes y suscriptores, la verificación y guarda de la documentación probatoria son realizadas por las Autoridades de Registro. Existe una Autoridad de Registro Central, operada por ENCODE S.A., y Autoridades de Registro Delegadas, las que son operadas por Organizaciones que, a dichos efectos, hayan convenido con ENCODE S.A. Estas autoridades de registro delegadas están bajo el control y supervisión de la Autoridad de Registro Central de ENCODE S.A. También las autoridades de registro podrán desarrollar su actividad en puestos móviles.
Las Autoridades de Registro habilitadas se publicarán en el sitio:

- https://www.encodesa.com.ar/autoridades-de-registro.html

1.3.3. Suscriptores de certificados

Según los términos de la presente Política Única de Certificación asociada al presente Manual, 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.

1.3.4. Terceros Usuarios

Son Terceros Usuarios de los certificados emitidos bajo la Política Única de Certificación asociada al presente Manual 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 correspondientes a los certificados digitales que se emitan bajo la Política Única de Certificación asociada al presente Manual podrán ser utilizadas en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado.

1.5. Administración del Manual de Procedimientos

1.5.1. Responsable del documento

El Manual de Procedimientos de Certificación es administrado por ENCODE S.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: (0) (351) 569 4407 o 569 4408 y líneas rotativas

1.5.2. Contacto

El responsable del registro, mantenimiento e interpretación del Manual de Procedimientos 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:

arc@encodesa.com.ar

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

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

1.5.3. Procedimientos de aprobación de la Política de Certificación

Según los establecido por la Ley 25.506, su Decreto Reglamentario Nº 182/2019 y modificatorios, las Resoluciones Nº 399 E/2016 y 213 E/2017 del ex Ministerio de Modernización, la resolución 86/2020 de la Secretaria de Innovación Pública, la
Política Única de Certificación de ENCODE S.A. y los documentos relacionados obligatorios, así como sus modificaciones, deben ser aprobados por el Ente Licenciante de Firma Digital de la República Argentina.

Este Manual de Procedimientos ha sido presentado ante el Ente Licenciante y ha sido aprobado por el correspondiente acto administrativo.

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

Se indican las definiciones de los conceptos relevantes utilizados en el presente documento:

Autoridad de Aplicación: La SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de Firma Digital en la REPÚBLICA ARGENTINA.
Autoridad de Registro: Es la entidad que tiene a su cargo las funciones de:

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.
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 emitidos por el certificador licenciado, 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 9 de la

Resolución MM N° 399/2016. 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 exclusivamente a las tareas de certificación.

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 Continuidad de las operaciones: Conjunto de procedimientos a seguir por el Certificador Licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

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

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.
CUIL: Clave Única de Identificación Laboral
DNFDIT: Dirección Nacional de Firma Digital e Infraestructura Tecnológica
IEC: International Electrotechnical Commission.
IETF: Internet Engineering Task Force.
MM: Ministerio de Modernización.
SIP: Secretarìa De Innovación Pública**OCSP:** Protocolo en línea del estado de un certificado ("On-line Certificate Status Protocol").
OID: Identificador de Objeto ("Object Identifier").
RFC: Request for Comments.

2. RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS

2.1. Repositorios

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

2.2. Publicación de información del certificador

Según lo descripto en "2.2. Publicación de información del certificador" de la Política Única de Certificación de ENCODE S.A.

2.3. Frecuencia de publicación

Según lo descripto en "2.3. Frecuencia de publicación" de la Política Única de Certificación de ENCODE S.A.

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 de este 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, e l 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.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Asignación de nombres de suscriptores

La descripción del registro inicial está contenida en “3.1. Asignación de nombres de suscriptores” de la Política Única de Certificación de ENCODE S.A. Es importante acceder y tomar conocimiento de ella, particularmente de la información que el solicitante debe consultar y tener presente antes de iniciar su solicitud.

3.1.1. Tipos de Nombres

No se establecen restricciones a los nombres que pueden ser incluidos dentro de los certificados, en tanto se correspondan con la documentación probatoria exigida para la emisión de certificados por la Política de Certificación asociada a este Manual.

3.1.2. Necesidad de Nombres Distintivos

La necesidad del uso de nombres distintivos está expuesta en “3.1.2. – Necesidad de Nombres Distintivos” de la Política Única de Certificación de ENCODE S.A.

3.1.3. Anonimato o uso de seudónimos

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

3.1.4. Reglas para la interpretación de nombres

Rige lo establecido en “3.1.4. Reglas para la interpretación de nombres” de la Política Única de Certificación de ENCODE S.A.

3.1.5. Unicidad de nombres

La Política Única de Certificación de ENCODE S.A cumple con lo indicado en la Resolución MM N° 399 E/2016 del ex Ministerio de Modernización en lo que respecta a la necesidad de que el nombre distintivo sea único en “3.1.5. Unicidad de nombres”.

Procedimiento de resolución de disputas sobre nombres

- **Frecuencia, oportunidad y urgencia**

Disponible en forma permanente. No planificado. Urgencia baja.

- **Roles que participan en el procedimiento**

a) Responsable de Firma Digital de ENCODE S. A.
b) Responsable de la AR Central.
c) Responsable de AR Delegada.
d) Solicitante.

- **Acción que pone en marcha el procedimiento**

Disputa o conflicto en la utilización de nombres para titulares de certificados de persona humana o de persona jurídica.

- **Tareas a realizar por cada uno de los roles que actúan**

a) El solicitante presenta su reclamo por nota ante el Responsable de la AR Central y/o el Responsable de la AR Delegada.
b) El Responsable de la AR Central o Responsable de la AR Delegada evalúa y convoca al Responsable de Firma Digital para tratar el reclamo.
c) Los roles intervinientes dirimen la disputa tomando como criterio lo establecido en: “3.1.4. – Reglas para la interpretación de nombres”, “3.1.5. – Unicidad de nombres” y “3.1.6. – Reconocimiento, autenticación y rol de las marcas registradas” de la Política Única de Certificación de ENCODE S.A.
d) El Responsable de Firma Digital resolverá lo que estime corresponder, conforme a criterios de máxima razonabilidad, equidad y pleno ajuste a la normativa vigente y aplicable en la especie.
e) El Responsable de la Central o Responsable de la AR Delegada comunica al correo electrónico informado oportunamente por el solicitante la resolución del reclamo.

- **Resultado del procedimiento**

Identificación de los campos a aplicar en el certificado digital, que conformarán el nombre único del titular y correo electrónico de comunicación de resolución al solicitante.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

Rige lo establecido en “3.1.6. Reconocimiento, autenticación y rol de las marcas registradas” de la Política Única de Certificación de ENCODE S.A.

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.

3.2.1. Métodos para comprobar la titularidad del par de claves

El método de comprobación está estrechamente ligado con la generación de la solicitud, dado que ambos se generan mediante un único procedimiento. Esto asegura que, si un solicitante generó y presentó una solicitud de certificado digital, él es poseedor de la clave privada.

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, utilizando su propio equipamiento. 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 en el equipo del solicitante y en ningún momento de la generación los sistemas informáticos de Encode 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, usando una computadora personal con la cual también genera la Solicitud, la clave privada quedará almacenada en su perfil de usuario y bajo su exclusivo control.
- En los casos en que el Solicitante utilizara un dispositivo criptográfico de su propiedad, las claves son generadas y almacenadas en él.
- En los casos en que el Solicitante utilizara un servicio de firma digital con custodia centralizada de claves criptográficas de Certificados, las claves son generadas, almacenadas y utilizadas en un dispositivo criptográfico FIPS 140-2 nivel 3.
- 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 y verifica automáticamente mediante un algoritmo de control la existencia de la correspondencia de la clave privada asociada a la clave pública incluida en este requerimiento al momento de su generación.
- En caso de ser correcto el formato, la aplicación del Certificador entrega al Solicitante una Solicitud completa incluyendo el resumen criptográfico.
- El Solicitante debe imprimir la Solicitud, para entregar en la Autoridad de Registro, cuando se presenta en el proceso de identificación, demostrando así la posesión de la clave privada.

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

Este proceso tiene como requisito previo la elaboración de la solicitud del certificado digital y la creación del par de claves criptográficas, son parte del Ciclo del certificado y se describen en “4.1.2. Solicitud de certificado para personas jurídicas”.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Planificado. Urgencia alta. Se realiza solo en horario laboral.

- **Roles que participan en el procedimiento**

a) Solicitante o suscriptor

b) Oficial de Registro

- **Acción que pone en marcha el procedimiento**

Presentación del solicitante ante el Oficial de Registro para acreditar fehacientemente su identidad y la de la persona jurídica.

- **Tareas a realizar por cada uno de los roles que actúan**

El Solicitante, en carácter de, responsable autorizado de la persona jurídica se presenta ante el Oficial de Registro, con la documentación necesaria, según lo especificado en la “Guía del Solicitante” que se encuentra publicada en el sitio del Certificador.

http://www.encodeac.com.ar/firma-digital/guia del solicitante.html

El Solicitante será atendido por el 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.

El Oficial de Registro revisará que:

El responsable autorizado 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 modo ilustrativo se mencionan algunos de los comprobantes a presentar):

- Estatuto o Contrato Social correspondiente a la Persona Jurídica.
- Acta de directorio o documento que acredite la representación invocada y su documento de identidad,
- Constancia de inscripción en el Registro Público de Comercio.
- Constancia de inscripción en AFIP.
- DNI de todos los socios, en caso de sociedades irregulares,
- Acta de distribución de cargos.
- 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.
- Solicitud de certificado impresa.
- Recibo que acredita el pago del certificado correspondiente.
- 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.encodeac.com.ar/firma-digital/guia del solicitante.html

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 veces para poder continuar con el procedimiento de identificación 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. El Oficial de Registro conserva para el armado de la

carpeta del suscriptor la documentación presentada como respaldo del proceso de identificación.

Recibida la documentación en la AR Central o AR Delegada, 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.

El Oficial de Registro procede a la guarda de la carpeta en un armario ubicado en el segundo nivel de seguridad de la AR correspondiente.

En caso de que uno o más documentos no cumplan los requisitos necesarios, existan dudas en cuanto a la validez de los documentos de identidad o la correspondencia entre el documento presentado y su titularidad, la documentación será devuelta al solicitante que deberá iniciar un nuevo proceso de identificación dentro del plazo de vigencia de su solicitud que es de TREINTA (30) días y presentar los documentos actualizados ante el Oficial de Registro correspondiente.

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, el Responsable de AR Central, AR Delegada u Oficial de Registro, podrá requerir, ante posibles cambios en el perfil del certificado respecto de la verificación realizada con anterioridad, que el Solicitante o Suscriptor se presente nuevamente para acreditar identidad.

- **Resultado del procedimiento**

a) En caso de aceptación:
   - Solicitud aprobada.
   - Acuerdo con Suscriptores firmado.
   - Carpeta de identificación del Solicitante o Suscriptor en la AR correspondiente.

b) En caso de rechazo:
   - Solicitud rechazada.

3.2.3. Autenticación de la identidad de Personas Humanas

Este proceso tiene como requisito previo la elaboración de la solicitud del certificado digital y la creación del par de claves criptográficas, son parte del Ciclo del certificado y se describen en “4.1.2. Solicitud de certificado”.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Planificado. Urgencia alta. Se realiza solo en horario laboral.

- **Roles que participan en el procedimiento**

    a. Solicitante o suscriptor
    b. Oficial de Registro

- **Acción que pone en marcha el procedimiento**

Presentación del Solicitante o Suscriptor persona humana ante el Oficial de Registro para acreditar fehacientemente su identidad.

- **Tareas a realizar por cada uno de los roles que actúan**

El solicitante presenta la siguiente documentación en original y copia:

a) Documento de Identidad (de poseer nacionalidad argentina, se requiere Documento Nacional de Identidad; de tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales) en original y duplicado de la primera y segunda hoja, firmada por el solicitante;
b) Código Único de Identificación Laboral (C.U.I.L.)
c) Constancia de inscripción en AFIP, si corresponde
d) Solicitud impresa.
e) Recibo que acredita el pago del certificado
f) Datos biométricos (el OR captura huella digital e imagen de rostro del solicitante)

A los fines que el Solicitante y todos los involucrados en el proceso de identificación tomen conocimiento de la documentación actualizada que requiere ser acompañada a los fines de la identificación de la persona humana, se sugiere consultar la “Guía del Solicitante” que se encuentra publicada en el sitio del Certificador: http://www.encodeac.com.ar/firma-digital/guia del solicitante.html

El Solicitante será atendido por el Oficial de Registro, quien verificará su identidad. El Oficial de Registro revisará que:

El documento de identidad presentado sea válido, que sea el mismo tipo y número que se

indicó en la solicitud de certificado y que la foto coincida con la persona que tiene enfrente.

El nombre de la persona humana que obra en la Solicitud sea el mismo que en la constancia de inscripción en AFIP y que el número de AFIP que figura en la Solicitud sea igual al de la Constancia.

El CUIL indicado en la solicitud es correcto, el cual ya ha sido validado a través de su algoritmo verificador al momento de 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 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 cumplas estas CUATRO (4) veces, para poder continuar con el procedimiento de reconcomiendo que tiene por finalidad dejar asociado al certificado una foto y una huella dactilar representativa de la persona.

Si la identificación ha sido aprobada, el Solicitante firma dos ejemplares impresos del

“Acuerdo con Suscriptores”, quedando uno en poder del Solicitante.

El Oficial de Registro devuelve los originales de todos los documentos al Solicitante y conserva los duplicados, como respaldo del proceso de identificación.

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, 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 humana Solicitante. Esta contiene la Solicitud de Certificado firmada, los duplicados de todos los documentos presentados y el Acuerdo con Suscriptores firmado.

En caso de que uno o más documentos no cumplan los requisitos necesarios, existan dudas en cuanto a la validez de los documentos de identidad o la correspondencia entre el documento presentado y su titularidad, la documentación será devuelta al solicitante que deberá iniciar un nuevo proceso de identificación dentro del plazo de vigencia de su solicitud que es de TREINTA (30) días y presentar los documentos actualizados ante el personal de la AR Central o personal de la AR Delegada.

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, el Responsable de AR Central, Responsable de la AR Delegada u Oficial de Registro, podrá requerir ante posibles cambios en el perfil del certificado respecto de la verificación realizada con anterioridad, que el Solicitante o

Suscriptor se presente nuevamente para acreditar identidad.

Resultado del procedimiento En caso de aceptación:

- Solicitud aprobada.
- Acuerdo con Suscriptores firmado.
- Carpeta de identificación del Solicitante/Suscriptor en la AR En caso de rechazo.
- Solicitud rechazada.
- Correo electrónico de notificación de rechazo.

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. de la Política Única de Certificación de ENCODE S.A., el Certificador Licenciado o la Autoridad de Registro con la que se encuentre operativamente vinculado, verifica la autorización de la Persona Humana que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente.

3.2.6. Criterios para la interoperabilidad

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

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

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

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

- después de la revocación de UN (1) certificado
- después de la expiración de UN (1) certificado
- antes de la expiración de UN (1) certificado

En los certificados de personas humanas, 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.

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."

En caso de que el suscriptor requiriera generar un nuevo par de claves después de

una revocación, deberá realizar el proceso de solicitud completo, incluyendo la generación de un nuevo par de claves y también el envío de la nueva solicitud y la presentación frente a la AR para validar su identidad.

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

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

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

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

3.4. Requerimiento de revocación

El requerimiento de revocación de los certificados digitales se describe en "3.4. Requerimiento de revocación" de la Política Única de Certificación de ENCODE S.A.

El requerimiento de revocación podrá ser iniciado por el Suscriptor o el Certificador Licenciado o la Autoridad de Registro operativamente vinculada, cuando se produzcan las causas indicadas en "4.9.1. Causas de revocación" de la Política Única de Certificación de ENCODE S.A.

Luego de hecho el requerimiento, deberá efectivizase la revocación, como se describe en "4.9. Suspensión y Revocación de Certificados".

Procedimiento para requerir la revocación

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Poco frecuente. No planificado. Urgencia muy alta.

- **Roles que participan en el procedimiento**

a) Suscriptor
b) Responsable de la AR Central
c) Responsable de la AR Delegada
d) Oficial de Registro
e) Autoridad Certificante del Certificador Licenciado de ENCODE S.A
f) La Autoridad de Registro
g) La Autoridad de Aplicación
h) La Autoridad Judicial competente

- **Acción que pone en marcha el procedimiento**

En el caso del Suscriptor, puede iniciar el proceso accediendo al sitio web correspondiente o presentarse ante la AR Central o AR Delegada para solicitarlo.

El responsable autorizado, si se trata de una persona jurídica, aplicación o sitio seguro, puede iniciar el proceso accediendo al sitio web correspondiente o presentarse ante la AR Central o AR Delegada para solicitarlo.

En caso de detección de alguna causa de revocación también podrán solicitarla:

- La Autoridad de Registro
- La Autoridad de Aplicación
- La Autoridad Judicial competente.
- El Certificador Licenciado.

ENCODE S.A. procederá a revocar un certificado en los siguientes casos:

a) Cuando lo solicite el titular del certificado por cualquier causa, incluida el haber tomado conocimiento de que su clave privada esté comprometida y haya dejado de ser segura.

b) Si ENCODE S.A. determina que el certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

c) Si ENCODE S.A. determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) En caso que la Organización que haya adoptado el uso de certificados de firma digital emitidos por la AC de ENCODE S. A., notifique a la Autoridad de Registro que la

e) información contenida en el certificado ha dejado de ser exacta.

f) Cuando fuere solicitado por resolución judicial o de la Autoridad de Aplicación de la Ley Nº 25.506 debidamente fundada.

g) Si ENCODE S.A. determina que el certificado dejó de cumplir con las políticas y normas legales y reglamentarias de la Infraestructura de Firma Digital de la República Argentina (IFDRA).

h) Por fallecimiento del titular, declaración judicial de ausencia con presunción de fallecimiento o declaración judicial de incapacidad, en el caso de persona humana comunicada fehacientemente por sus herederos o autoridad judicial competente a ENCODE SA.

i) Por cese del responsable autorizado, en el caso de personas jurídicas comunicada

j) fehacientemente por el nuevo responsable autorizado de la persona jurídica a ENCODE S.A.

k) Por cambio en los atributos de un certificado, aun cuando hubieran sido válidos al tiempo de su emisión.

l) Por cese de la existencia de la Persona Jurídica, comunicada fehacientemente por el responsable autorizado de la misma a ENCODE S.A.

m) Por cese de la Licencia del Certificador.

n) Por haberse resuelto el contrato que ENCODE S.A. hubiera suscripto con la Organización a la cual perteneciese el Suscriptor, o lo convenido entre las partes, en el caso que corresponda.

- **Tareas a realizar por cada uno de los roles que actúan**

Revocación por PIN

a) 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 está disponible SIETE (7) días de la semana, las 24 horas, los TRESCIENTOS SESENTA Y CINCO (365) días del año.

b) En el caso que el suscriptor no contara con el PIN, lo podrá solicitar en el portal del suscriptor. La aplicación, en forma automática, le devolverá en su correo electrónico al suscriptor, el PIN para que pueda realizar la revocación.

c) El suscriptor que inicia la revocación se debe identificar en la aplicación con su CUIL

o CUIT y su Clave o PIN de revocación, y procede a enviar la solicitud de revocación, la que es procesada de inmediato.

Revocación en Autoridad de Registro

a) En caso que el suscriptor se presente ante la Autoridad de Registro, ésta controlará las causas de revocación manifestadas por el suscriptor y en caso de que presente documentación, el Oficial de Registro efectuará copia de la misma.

b) En caso de tratarse de personas o entidades habilitadas para solicitar la revocación, como la Autoridad de Aplicación o autoridad judicial competente que no cuentan con el PIN de revocación correspondiente, deberán comunicarse a los contactos establecidos por ENCODE S.A. en “1.5.2. Contacto” de la Política Única de Certificación de ENCODE S.A., para solicitar la revocación al Responsable de la Autoridad de Registro mediante notificación fehaciente u oficio judicial.

En todos los casos enunciados en este punto se dejará constancia en los

registros de la aplicación de la Autoridad de Registro, el motivo de la revocación y la misma será autorizada por el Responsable Legal de ENCODE S.A.

c) El suscriptor firma la copia de la documentación que entrega al Oficial de Registro.

d) El Oficial de Registro firma la documentación recibida.

e) En la aplicación de la AR seleccionará la solicitud correspondiente al certificado que se autoriza revocar y generará el requerimiento en la aplicación.

f) El suscriptor recibirá un correo electrónico de la aplicación informando la revocación del certificado.

g) La Autoridad de Registro es notificada por la aplicación para hacer el proceso de registro y archivo como respaldo de la acción realizada.

En los casos de que no se pueda verificar las condiciones para proceder a la revocación, la solicitud de revocación será rechazada, comunicándose dicha situación al correo electrónico informado por el suscriptor al momento de la solicitud.

- **Resultado del procedimiento**

En caso de verificar las condiciones para una revocación

- Pedido de Revocación solicitada.
- Notificación de la revocación al Solicitante.
- Notificación de la revocación a la AR.
- Envío de PIN de revocación, si corresponde.

En caso de no poder verificar las condiciones para una revocación

- Solicitud de Revocación Rechazada
- Correo de notificación de Solicitud de revocación Rechazada

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de Certificado

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

4.1.1. Solicitantes de certificados

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

4.1.2. Solicitud de Certificado

Se detallan los procedimientos de solicitud de certificado.

Esos requerimientos incluyen acreditación de identidad, clave de acceso, estación de trabajo con configuración adecuada y dispositivo criptográfico de propiedad del suscriptor.

a) Personas Humanas

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

- **Roles que participan en el procedimiento**

Solicitante.

- **Acción que pone en marcha el procedimiento**

Acceso del Solicitante al sistema, acreditando su identidad.

- **Tareas a realizar por cada uno de los roles que actúan**

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 de persona humana, 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/guia del solicitante.html
- En caso de contar el Solicitante con un dispositivo criptográfico propio, de los modelos validados por el Certificador deberá colocarlo 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 como también se deberá cumplir con el uso de dispositivo criptográfico FIPS 140-2 Level 3), cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.
- La aplicación a continuación desplegará la Autoridad de Registro Central y las Autoridades de Registro Delegadas y/o móviles, debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación.
- 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.
- El Solicitante recibe en el mail informado el pedido de confirmación y lo abre y envía la confirmación a la aplicación de solicitud.
- Únicamente al ser confirmada la recepción del correo electrónico la aplicación le mostrara la continuación del formulario de Solicitud.
- La aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generará el par de claves criptográficas asimétricas.

- Al elegir el proveedor, el solicitante elige también si la generación es por software o por hardware, y si es con custodia centralizada de claves criptográficas.

  En caso de elección por software, las claves deben ser resguardadas con un pin de seguridad para su acceso.

  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 modelos validados por ENCODE S.A. El suscriptor deberá establecer la clave de acceso al dispositivo criptográfico. Las claves de los suscriptores que cuenten con dispositivos criptográficos externos removibles deberán estar protegidas por dos factores de seguridad:

  1. mediante la posesión del dispositivo por el suscriptor.
  2. la contraseña de la clave privada definida por el propio suscriptor. En el caso de elección de 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.

- 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. A continuación, podrá enviar 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 del certificado.
- 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 este hecho al Solicitante, en su dirección de correo electrónico.
- El proceso continúa como se describe en “3.2.3. Autenticación de la identidad de persona humana” y de resultar satisfactorio en “4.3. Emisión del certificado”.

➢ **Resultado del procedimiento**

Si fue exitoso:

- El Solicitante generó el par de claves criptográficas.

- La aplicación generó la solicitud pendiente de verificación.
- El Sistema le envió al Solicitante un recordatorio para el proceso de identificación.

Si se rechazó:

- El Solicitante fue notificado respecto al rechazo de su Solicitud.

b) Personas Jurídicas, sitios seguros o de aplicación.

➢ **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

➢ **Roles que participan en el procedimiento**

- Solicitante, persona jurídica iniciado a través de su representante, administrador o apoderado.

➢ **Acción que pone en marcha el procedimiento**

Acceso del solicitante en su carácter de representante legal, administrador o apoderado al sistema, acreditando su identidad y el registro los datos de la persona jurídica solicitante.

➢ **Tareas a realizar por cada uno de los roles que actúan**

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el representante legal, administrador o apoderado 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. En caso de Solicitud del certificado sitio seguro deberá seleccionar la opción de “Certificados SSL” para sitio seguro o “Certificados de aplicaciones” para aplicación.
- Contar con su dirección de correo electrónico propia y exclusiva del solicitante 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

  softwares detallados en la “Guía del Solicitante” que se encuentra en:

  http://www.encodeac.com.ar/firma-digital/guia del solicitante.html

- El proceso de solicitud podrá ser iniciado solamente por responsable autorizado de la persona jurídica a favor de la cual se emitirá el certificado, ingresando al Portal del Suscriptor.

- La aplicación del Certificador verifica que la estación de trabajo del Solicitante cumple con los requerimientos técnicos mínimos.
- En caso de contar el Solicitante con un dispositivo criptográfico propio, deberá colocarlo al inicio de la sesión.
- En caso de utilizar un servicio de firma digital con custodia centralizada de claves criptográficos, éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado (como también se deberá cumplir con el uso de dispositivo criptográfico FIPS 140-2 nivel 3), 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 sistema a continuación desplegará la Autoridad de Registro Central, la Autoridades de Registro Delegadas y/o móviles, si correspondiere, debiendo el Solicitante proceder a elegir libremente la opción más conveniente a los efectos de completar su identificación.
- 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.
- El Solicitante recibe en el mail informado el pedido de confirmación y lo abre y envía la confirmación a la aplicación de solicitud.
- Únicamente al ser confirmada la recepción del correo electrónico la aplicación le mostrara la continuación del formulario de Solicitud.
- 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, se debe contar con la clave de acceso al dispositivo criptográfico y podrá realizar la generación en el mismo. En caso contrario la generación se hará por software. Cuando se genere por software las claves deben ser resguardadas con un pin de seguridad para su acceso.
- 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, en los casos que corresponda se le informará importe y formas de pago disponibles.
- 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.

➢ **Resultado del procedimiento**

Si fue exitoso:

- El Solicitante generó el par de claves criptográficas.
- La aplicación generó la solicitud de certificado de persona jurídica pendiente de identificación.
- Se informó al Solicitante el pin de revocación.
- El Sistema le envió al Solicitante un recordatorio para el proceso de identificación.

Si fue rechazado:

- Se informa al Solicitante que no se generó su Solicitud.

4.2. Procesamiento de la solicitud del certificado

Los requerimientos están detallados en “4.2. Procesamiento de la solicitud del certificado” de la Política Única de Certificación de ENCODE S.A.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

- **Roles que participan en el procedimiento**

a) Solicitante titular persona humana o persona jurídica, iniciado a través de su responsable autorizado.

- **Acción que pone en marcha el procedimiento**

Acceso del solicitante acreditando su identidad y el registro los datos de la persona humana o jurídica solicitante.

- **Tareas a realizar por cada uno de los roles que actúan**

El proceso de solicitud de emisión de certificado debe ser iniciado por el Solicitante, quien luego deberá acreditar fehacientemente su identidad.

a) Solicitud de certificado de persona humana

- El proceso continúa como se describe en “3.2.3. Autenticación de la identidad de Personas Humanas” del presente documento.
- 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.

b) Solicitud de certificado de persona jurídica

- El proceso continúa como se describe en “3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas” del presente documento.
- 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.

c) 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. Toda esta información, incluido el registro biométrico del Solicitante, se almacena digitalmente en la aplicación de la Autoridad de Registro.

➢ **Resultado del procedimiento**

Si fue exitoso:

- Aprobación de la Solicitud.
- Carpeta de identificación del suscriptor almacenada. Si fue

rechazado:

- Se informa al Solicitante el rechazo de su Solicitud.

4.3. Emisión del certificado

Para cualquier tipo de certificado, se emite y se coloca en el portal del suscriptor, luego de cumplido el proceso de identificación y autenticación y aprobada la Solicitud de emisión de certificado o la Solicitud de renovación de certificado por la Autoridad de Registro y abonado el arancel de emisión y/o renovación.

El Portal del Suscriptor se encuentra en:

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

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

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

- **Roles que participan en el procedimiento**

a) Autoridad Certificante ENCODE S.A.

- **Acción que pone en marcha el procedimiento**

Información ingresada por la Autoridad de Registro sobre aprobación de la solicitud y pago del arancel.

- **Tareas a realizar por cada uno de los roles que actúan**

La aplicación de la Autoridad Certificante verifica la firma digital de la aprobación realizada por la Autoridad de Registro a la Solicitud de emisión.

La aplicación de la Autoridad Certificante remite el requerimiento con la clave pública del solicitante, en formato PKCS#10, al Servicio de Certificación de la Autoridad Certificante.

El Servicio de Certificación de la Autoridad Certificante ENCODE S.A. emite el correspondiente certificado, firmándolo digitalmente con su clave privada.

La aplicación del Certificador coloca el certificado en el Portal del Suscriptor, a disposición de su titular.

El Portal del Suscriptor se encuentra en: http://www.encodeac.com.ar/firma- digital/portal-suscriptor.html

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

Le comunica al Solicitante o Suscriptor la disponibilidad de su certificado por correo electrónico y se le informa el PIN de revocación.

La aplicación de la Autoridad Certificante, una vez que se emitió el certificado, eliminará automáticamente el requerimiento PKCS#10 asociado a ese certificado con el fin de evitar que se genere un nuevo certificado con dicho requerimiento.

El proceso continúa con “4.4. Aceptación del Certificado”.

- **Resultado del procedimiento**

Se emitió el certificado, firmado con la clave privada de la Autoridad Certificante ENCODE S.A, y se lo puso a disposición del solicitante que se convierte en suscriptor.

4.4. Aceptación del certificado

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia baja.

- **Roles que participan en el procedimiento**

Suscriptor

- **Acción que pone en marcha el procedimiento**

Aviso de emisión del certificado, enviado por la aplicación del Certificador y recibido por el suscriptor.

- **Tareas a realizar por cada uno de los roles que actúan**

El Portal del Suscriptor se encuentra en: http://www.encodeac.com.ar/firma- digital/portal-suscriptor.html

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

El suscriptor descarga su certificado desde el portal, almacenándolo en el dispositivo criptográfico si dispone de él o en el disco de su computador.

El suscriptor debe controlar el contenido del certificado.

Si el contenido es incorrecto debe revocar el certificado con su PIN de revocación desde el mismo portal o en caso contrario informar de inmediato sobre cualquier error a la Autoridad de Registro que aprobó la solicitud, para que ésta solicite en forma urgente la 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 de la puesta a disposición en el portal del suscriptor del certificado a su nombre

Si no se encuentra ni comunica error, se entiende que el certificado es correcto. 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 la Política Única de Certificación de ENCODE S.A.

- **Resultado del procedimiento**

Certificado aceptado en poder del suscriptor, en condiciones de ser usado según lo especificado en la Política Única de Certificación de ENCODE S.A.

Si los datos son incorrectos, el Certificado es revocado.

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

Las responsabilidades y limitación del uso del par de claves y del certificado, se establecen en la Política Única de Certificación de ENCODE S.A.

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 Política Única de Certificación de ENCODE S.A.;

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.

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.

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.
h) La autoridad judicial competente.
i) La Autoridad de Aplicación.

4.9.3 Procedimientos para la solicitud de revocación

Para solicitar la revocación de un certificado, se seguirá lo indicado en "3.4. Requerimiento de revocación".

En el presente punto se trata el procesamiento de esa solicitud, a los efectos de materializar la revocación solicitada.

- **Frecuencia, oportunidad y urgencia**

Revocación por PIN

a) 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 está disponible SIETE (7) días de la semana, las 24 horas, los TRESCIENTOS SESENTA Y CINCO (365) días del año.

b) En el caso que el suscriptor no contará con el PIN, lo podrá solicitar en el portal del suscriptor. La aplicación, en forma automática, le devolverá en su correo electrónico al suscriptor, el PIN para que pueda realizar la revocación.

c) El suscriptor que inicia la revocación se debe identificar en la aplicación con su CUIL o CUIT y su Clave o PIN de revocación, y procede a enviar la solicitud de revocación, la que es procesada de inmediato.

Revocación en Autoridad de Registro

a) En caso que el suscriptor se presente ante la Autoridad de Registro, ésta controlará las causas de revocación manifestadas por el suscriptor y en caso de que presente documentación, el Oficial de Registro efectuará copia de la misma.
b) Datos biométricos (el OR captura huella digital e imagen de rostro del solicitante)
c) En caso de tratarse de personas o entidades habilitadas para solicitar la revocación, como la Autoridad de Aplicación o Autoridad Judicial competente que no cuentan con el PIN de revocación correspondiente, deberán comunicarse a los contactos establecidos por ENCODE S.A. en "1.5.2. Contacto" de la Política Única de Certificación de ENCODE S.A., para solicitar la revocación al Responsable de la Autoridad de Registro mediante notificación fehaciente u oficio judicial.

En todos los casos enunciados en este punto se dejará constancia en los registros de la aplicación de la Autoridad de Registro, el motivo de la revocación y la misma

será autorizadas por el Responsable Legal de ENCODE SA.

d) El suscriptor firma la copia de la documentación que entrega al Oficial de Registro.

e) El Oficial de Registro firma la documentación recibida.

f) En la aplicación de la AR seleccionará la solicitud correspondiente al certificado que se autoriza revocar y generará el requerimiento en la aplicación.

g) El suscriptor recibirá un correo electrónico de la aplicación informando la revocación del certificado.

h) La Autoridad de Registro es notificada por la aplicación para hacer el proceso de registro y archivo como respaldo de la acción realizada.

En los casos de que no se pueda verificar las condiciones para proceder a la revocación, la solicitud de revocación será rechazada, comunicándose dicha situación al correo electrónico informado por el suscriptor al momento de la solicitud.

- **Resultado del procedimiento**

Certificado digital revocado, de acuerdo con la solicitud.

La AR Central o AR Delegada conservará como documentación probatoria la solicitud de revocación y el material probatorio vinculado.

La revocación se reflejará en la próxima Lista de Certificados Revocados, cuando sea generada de acuerdo con lo especificado en “2.3. Frecuencia de publicación”.

4.9.4 Plazo para la solicitud de revocación

La recepción de la solicitud de revocación está disponible SIETE POR VEINTICUATRO (7 x 24) hs. a través de la aplicación del Certificador desde:

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

Esta solicitud será procesada de inmediato, sin intervención de la Autoridad de Registro.

En caso que el suscriptor se presente ante la AR Central o AR Delegada, esta controlará las causas de revocación manifestadas por el suscriptor y en caso de que presente documentación, el Oficial de Registro realizará un duplicado de la documentación presentada

El Oficial de Registro verificará que se cumplan las condiciones para realizar una solicitud de revocación.

En la aplicación de la AR el Oficial de Registro seleccionará la solicitud correspondiente al certificado que se autoriza revocar y generará el requerimiento en la aplicación.

El Oficial de Registro asentará en los registros de la aplicación de la AR el requerimiento de

revocación.

El Suscriptor recibirá un correo electrónico de la aplicación informando la revocación del certificado.

4.9.5 Plazo para el procesamiento de la solicitud de revocación

Según se establece en “4.9.5. Plazo para el procesamiento de la solicitud de revocación” de la Política Única de Certificación de ENCODE S.A.

4.9.6 Requisitos para la verificación de la lista de certificados revocados

Según se establece en “4.9.6. Requisitos para la verificación de la lista de certificados revocados” de la Política Única de Certificación de ENCODE S.A.

4.9.7 Frecuencia de emisión de listas de certificados revocados

La Autoridad Certificante 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

La Autoridad Certificante 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.

4.9.10 Requisitos para la verificación en línea del estado de revocación

Para determinar el estado de validez de un certificado, se debe obtener la CRL vigente, verificar su integridad controlando la validez de su firma y constatar la inclusión o no del certificado en cuestión.

En los repositorios descriptos en “2.2. Publicación de información del certificador” de la Política Única de Certificación, se conserva únicamente la última CRL emitida. Las versiones de CRLs emitidas previamente son mantenidas en los archivos internos del Certificador

Si no se pudiera obtener una CRL actualizada, quien busca la verificación deberá optar entre rechazar el documento firmado digitalmente, aceptarlo bajo exclusiva responsabilidad de quien consulta o postergar la decisión hasta obtener una CRL actualizada.

Todas las aplicaciones habilitadas para el uso de los certificados emitidos por AC ENCODE S.A. cuentan con servicio de verificación automática de los certificados.

Las aplicaciones habilitadas por ENCODE S.A se encuentran publicadas en la url:

http://www.encodeac.com.ar/firma-digital/aplicaciones.pdf

Las mismas verifican en forma automática el estado de validez de los certificados utilizados por los suscriptores.

4.9.11 Otras formas disponibles para la divulgación de la revocación

Los mecanismos válidos para la verificación del estado de los certificados son a través de las Listas de Certificados Revocados y el Servicio OCSP.

Se utiliza el protocolo OCSP (On-Line Certificate Status Protocol) que permite, mediante su consulta implementada conforme a lo previsto por la Resolución MM 399 E/2016 y lo indicado en la especificación RFC 6960, 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.

Estas claves utilizadas por OCSP son claves RSA con un tamaño mínimo de 4096 bits.

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.

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

Según se establece en “4.10.1. Características técnicas” de la Política Única de Certificación de ENCODE S.A.

4.10.2 Disponibilidad del servicio

Según se establece en “4.10.2. Disponibilidad del servicio” de la Política Única de Certificación de ENCODE S.A.

4.10.3 Aspectos operativos

No existen otros aspectos a mencionar además de los establecidos en los puntos anteriores.

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 la Política Única de Certificación asociada a este Manual 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

5.1 Controles de seguridad física

Los sistemas centrales de la Autoridad Certificante se encuentran en el Sitio de Máxima Seguridad (SMS) de ENCODE S.A., el cual cuenta con controles de seguridad física que protegen las instalaciones informáticas de la Autoridad Certificante ENCODE S.A y garantizan la continuidad de sus operaciones.

Más información se encuentra en el documento “Plan de Seguridad”.

5.2 Controles de Gestión

Los controles funcionales son realizados por personal de ENCODE S.A. sobre todos los roles que componen la Autoridad Certificante ENCODE S.A, verificando el cumplimiento de las responsabilidades de cada uno de ellos, de acuerdo a lo establecido en la Política Única de Certificación de ENCODE S.A. y en los documentos: “Roles y Funciones” y “Guía de instalación y funcionamiento de las Autoridades de Registro”.

Los roles son asignados por el Responsable de ENCODE S.A., respetando los siguientes criterios:

a) Cada uno de los roles tiene un titular asignado y un sustituto.

b) Los roles son asignados a personal que cumple funciones en ENCODE S.A., excepto en el caso las Autoridades de Registro Delegadas que son asignadas por las Organizaciones y aprobados por ENCODE S.A.”

En el caso de la Autoridad Certificante, las AR Delegadas, la AR Central se realizan controles funcionales, verificando el cumplimiento de las responsabilidades y procedimientos:

- La información de la solicitud ingresada por el Solicitante y la aprobación en la base de datos se encuentra firmada digitalmente por el Oficial de Registro de la Autoridad de Registro respectiva, impidiendo cualquier intento de manipulación de datos.
- Las firmas digitales de las Autoridades de Registro son verificadas por las aplicaciones de la Autoridad Certificante, como paso previo a la emisión de un certificado.
- Las Autoridades de Registro deben verificar los atributos unívocos de la solicitud (tipo y número de documento) junto con el resto de la información.
- Las Autoridades de Registro son responsables de cotejar los datos de la solicitud con la información obrante en sus registros y la documentación de respaldo.
- Se realizan revisiones periódicas para cotejar las solicitudes y los certificados emitidos con la documentación de respaldo correspondiente.

- Previo a la emisión, las aplicaciones de la Autoridad Certificante verifican la congruencia entre la información de la solicitud y del certificado.
- Antes de la puesta en producción de una nueva versión de las aplicaciones de la Autoridad Certificante, personal de ENCODE S. A. somete al sistema a pruebas de aceptación que determinan la confiabilidad del producto.
- Los servidores de la Autoridad Certificante son monitoreados para asegurar que no se incluyeron o reemplazaron archivos no autorizados dentro del sistema.

- La información de solicitudes y aprobaciones de la base de datos se encuentra firmada digitalmente por la Autoridad de Registro respectiva, impidiendo cualquier intento de manipulación de datos. Las firmas digitales de las Autoridades de Registro son verificadas por las aplicaciones de la Autoridad Certificante como paso previo a la emisión de un certificado.
- Se registran “logs” de todos los accesos y transacciones de la base de datos.
- Existen controles de consistencia sobre la base de datos que permiten determinar si la información es completa y correcta.
- Las aplicaciones de la Autoridad Certificante son monitoreadas constantemente y se envían mensajes de alerta.
- La Mesa de Ayuda de ENCODE S. A. está capacitada para asistir a todos los suscriptores y puede contactarse mediante correo electrónico o por teléfono, tal como se describe en el documento Política Única de Certificación de ENCODE S.A.
- El sistema es monitoreado constantemente y se envían mensajes de alerta.

- Si una alerta no puede ser resuelta en un plazo de VEINTICUATRO (24) horas, se trasladan las operaciones al sitio de contingencia.
- En caso que el rol de Responsable Técnico detecte problemas en el HSM que no puedan ser resueltos en el plazo de DIECISEIS (16) horas se trasladan las operaciones al sitio de contingencia.
- La emisión de las CRLs es monitoreada por el servicio de monitoreo, que notifica por correo electrónico a su| responsable de monitoreo, novedades y alertas.
- La información de cada CRL es cotejada con la CRL precedente.
- Se realizan revisiones periódicas para cotejar que todos los certificados revocados estén incluidos en la CRL correspondiente.

5.3 Controles de seguridad del personal

Los controles de seguridad del personal que desempeña los roles que componen la Autoridad Certificante ENCODE S.A, serán los establecidos por ENCODE S.A. e

implementados a través de su Responsable de Recursos Humanos. Se efectúa un previo análisis y seguimiento de los antecedentes laborales del personal a través de su "Curriculum - Vitae" y evalúa la idoneidad del aspirante mediante una valoración psicotécnica. Además, ENCODE S.A. realiza una evaluación anual del desempeño de todo su personal.

En el caso de las Autoridades de Registro Delegadas, será responsabilidad de las Organizaciones mantener actualizado un legajo de antecedentes laborales, calificaciones profesionales, experiencia e idoneidad, para evaluar el desempeño del personal que cumpla

funciones como Oficiales de Registro. ENCODE S.A. realizará los controles pertinentes, comunicando a la Organización la realización y resultado de ellos.

a) Antecedentes laborales, calificaciones, experiencia e idoneidad del personal

Para cada persona vinculada con los servicios de certificación, ENCODE S.A. confecciona un legajo de antecedentes laborales, calificaciones profesionales, experiencia e idoneidad.

Todos los antecedentes personales y profesionales son evaluados antes de la asignación de una persona a un rol en estos servicios por el Responsable de la Autoridad Certificante y el Responsable de Recursos Humanos. Participará también el Responsable de la Autoridad de Registro Central cuando se trate de personal para el rol de Oficial de Registro.

En el caso de las Autoridades de Registro Propias de ENCODE en Empresas, la evaluación de los antecedentes personales y profesionales se llevará a cabo en conjunto entre el Responsable de la Autoridad de Registro Central y el responsable que designe la Empresa.

Todo el personal de la Autoridad Certificantes de ENCODE S.A. cumple o ha cumplido un Proceso de Selección previo a su incorporación que provee una razonable seguridad acerca de la confiabilidad y competencia de su personal para el adecuado cumplimiento de sus roles y funciones y que incluye los siguientes controles:

- El Responsable de Recursos Humanos de ENCODE S.A. conserva los certificados de falta de antecedentes penales de los candidatos (Certificados de Buena Conducta) en los correspondientes legajos del personal. Sólo son considerados quienes no poseen ningún antecedente negativo. También conserva constancia de los antecedentes de competencia, idoneidad y laborales de los candidatos en los correspondientes legajos de personal y en los sistemas de evaluación de desempeño, conforme a los requisitos establecidos para la contratación o designación en los regímenes aplicables.
- El Responsable de Recursos Humanos de ENCODE S.A. verifica de la aptitud de los candidatos mediante el chequeo de los antecedentes y referencias presentadas, entrevistas personales u otros mecanismos de selección adecuados para su precalificación.

- La selección entre los candidatos que hayan aprobado la prueba de aptitud del punto precedente está a cargo del Responsable de la Autoridad Certificante ENCODE S.A y el Responsable de Firma Digital de ENCODE S.A.
- Finalizado el Proceso de Selección, los candidatos seleccionados son contratados o designados en los roles respectivos por el Responsable de la Autoridad Certificante ENCODE S.A.
    - El Responsable de Recursos Humanos de ENCODE S.A. comunica por escrito el nombramiento a cada uno de los interesados y les hace firmar un “Acuerdo de Confidencialidad”.
- Toda la documentación de este proceso de selección, incluidos los “Acuerdos de Confidencialidad” oportunamente firmados son conservados en los archivos de la Autoridad Certificante ENCODE S.A. bajo la custodia del Responsable de Seguridad Informática.

b) Antecedentes laborales

- Análisis y evaluación de los Certificados de Buena Conducta, laboral y personal presentados por los candidatos.
- Comprobación de integridad y veracidad de la Hoja de Vida (Currículum Vitae) de los aspirantes.
- Constatación de las aptitudes académicas y profesionales de los aspirantes obrantes en sus respectivas Hojas de Vida, según corresponda.
- Verificación de la identidad de los aspirantes mediante la inspección de sus respectivos DNI o Pasaportes, según corresponda.
- Verificación de Crédito, cuando corresponda, a partir del análisis y evaluación de los informes pertinentes.

c) Entrenamiento y capacitación inicial

ENCODE S.A. realiza cursos de entrenamiento e instrucción en todas las políticas y procedimientos que conforman los manuales operativos de la Autoridad Certificante ENCODE S.A, como así también ante cambios en la tecnología de firma digital o en las plataformas utilizadas.

El personal de ENCODE S.A. es capacitado para poder cumplir con las funciones del rol asociado.

Los contenidos básicos se centrarán, entre otros, en los siguientes puntos relevantes:

- Infraestructura de firma digital.
- Responsabilidades y compromisos del rol y sus funciones.

- Procedimientos y políticas operacionales y de seguridad relacionadas con la AR Uso y operaciones de hardware y software empleado en las ARs.
- Manejo de incidentes y compromisos en materia de seguridad.
- Procedimientos de recuperación ante desastres y manejo de la contingencia para la continuidad de actividades de la AR.
- Gestión de la documentación inherente al funcionamiento de la AR.

Se llevará registro de los asistentes a la capacitación como de los resultados de la misma.

Se extenderán certificaciones de la capacitación.

d) Frecuencia de procesos de actualización técnica

Conforme se producen cambios en la tecnología de firma digital, en las plataformas utilizadas por la Autoridad Certificante o en sus procedimientos, ENCODE S.A. elabora programas de capacitación específicos para todo el personal afectado.

La capacitación será realizada al menos UNA (1) vez al año, siendo evaluado el personal afectado y otorgándose certificación cuando así correspondiere.

Los cursos de actualización técnica serán extensivos a las Autoridades de Registro Delegadas y ENCODE S. A. los coordinará con los Responsables de las Organizaciones.

El Responsable de la Autoridad Certificante,

Comunicará al personal de ENCODE en forma periódica novedades en materia de tecnología de firma digital, en las implementaciones referidas a infraestructuras de clave pública o en materia de seguridad informática, si así lo requieren.

Evaluará en forma conjunta con los responsables de las otras áreas de ENCODE la factibilidad y beneficios de la implementación de novedades tecnológicas.

Asesorará a la máxima autoridad de ENCODE sobre los beneficios de los cambios propuestos.

e) Frecuencia de rotación de cargos

No existe rotación entre los distintos cargos de la Autoridad Certificante

Esto es extensivo a las Autoridades de Registro e incluye a las Autoridades de Registro Delegadas.

f) Sanciones a aplicar por acciones no autorizadas

Constatada la infracción o incumplimiento de la Política Única de Certificación de ENCODE

S.A. acordada y o cualquier otra vulneración a los compromisos asumidos por el personal que desempeña los roles que componen la Autoridad Certificante y Autoridad de Registro de ENCODE S.A, se labrará el acta correspondiente, dejándose constancia de la fecha, hora y causa de la infracción y o incumplimiento.

Se comunicará el incumplimiento o infracción que se imputa, y se establecerá la sanción

definitiva. Se notificará de modo fehaciente al acusado de la infracción. La sanción definitiva podrá ser la desvinculación de la persona de ENCODE S.A.

Durante el período de análisis del incumplimiento, la persona no podrá cumplir funciones en las áreas sensibles de la Autoridad Certificante ni de la Autoridad de Registro Central y le serán retiradas todas las autorizaciones de acceso físico y lógico.

En el caso de incumplimientos comprobados del personal de Autoridades de Registro Delegadas, las sanciones por acciones no autorizadas posibles a aplicar son, entre otras:

- Revocación del Certificado Digital de los Oficiales de Registro de la Autoridad de Registro Delegada.
- Suspensión o inhabilitación como Autoridad de Registro Delegada.
- Resolución de lo convenido entre ENCODE S. A. y la Organización.

Toda sanción a aplicar se comunicará a los interesados en un plazo no mayor a DOS (2) días desde el momento de resolución de aplicación.

En caso de apreciarse mala fe en la utilización de los recursos informáticos de ENCODE S.A. principalmente aplicaciones y/o datos – ENCODE S.A. ejercerá las acciones que legalmente le amparen para la protección de sus derechos y sus recursos informáticos.

a) En el caso de detectase una conducta susceptible de ser constitutiva de infracción quien lo detecte, lo comunicará inmediatamente al Responsable de Seguridad Informática.

b) En el plazo de TRES (3) días el Responsable de Seguridad Informática calificará la gravedad de la infracción y,
   - Si estimase que se trata de una falta leve acordará sin más trámite la imposición de la correspondiente sanción.
   - Si estimase que se trata de una infracción grave o muy grave, lo comunicará inmediatamente al Responsable de Firma Digital y Responsable de Recursos Humanos.

c) Tratándose de una infracción grave o muy grave el Responsable de Recursos Humanos instruirá el correspondiente expediente, del cual se dejará constancia por escrito, en el cual:
   - Oirá al Responsable que hubiera realizado la comunicación y en su caso, al

trabajador afectado.

- Resolverá, previo asesoramiento técnico oportuno, sobre si la

  conducta es o no sancionable, y, en el primer caso, procederá a determinar su gravedad atendiendo a:

  - El mayor o menor grado de responsabilidad del trabajador.
  - Su categoría profesional.
  - La repercusión que la conducta infractora tenga en la empresa.

- Toda resolución que acuerde la imposición de una sanción deberá ser motivada, y en ella se explicitarán los datos del lugar donde ocurrió, del trabajador sancionado y una descripción completa de la infracción (lugar fecha y hora, descripción de la conducta y circunstancias determinantes de su gravedad).

d) La notificación de la sanción se realizará siempre por medio fehaciente, que deje constancia tanto del hecho de la notificación, como de su contenido.

Si se realiza de forma presencial, la copia de la notificación deberá ser firmada por el trabajador con expresión de la fecha en que se le efectúa la misma.

En otro caso, se efectuará por medio de telegrama con acuse de recibo o medio similar. Se evitarán aquellos sistemas que no dejen constancia del contenido de la notificación.

e) Cuando se impusiere una sanción muy grave se informará a la Máxima Autoridad de ENCODE S.A.

f) La valoración de las faltas y las correspondientes sanciones impuestas por la dirección de la empresa serán siempre revisables ante la jurisdicción competente.

g) Requisitos para contratación de personal

El personal a ser contratado a los efectos de cumplir acciones en servicio de certificación digital del Certificador Licenciado en el marco de su Política Única de Certificación de ENCODE S.A. deberá tener el conocimiento y formación suficiente para el mejor cometido de las funciones asignadas. Para ello, ENCODE S.A. llevará a cabo los procesos de selección de personal y capacitación que estime necesarios con el objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

En el caso de las Autoridades de Registro Delegadas, los procesos serán establecidos por la

Organización, los cuales deberán contemplar y respetar los requisitos mínimos del perfil laboral requerido para desempeñar el rol de Oficial de Registro, indicados en el documento “Guía de instalación y funcionamiento de las Autoridades de Registro”.

El proceso de selección de personal de ENCODE S.A. está a cargo del área de Recursos Humanos y consta de las siguientes actividades:

- Convocatoria
    - Elaborar en forma conjunta con el Área solicitante (es decir, la que necesita cubrir cargos vacantes) la Convocatoria con la siguiente información:
        - Tipo de Convocatoria
        - Información del cargo (denominación, grado, código, remuneración, etc.)
        - Ubicación orgánica y jerárquica del Rol
        - Número de vacantes a cubrir
        - Requisitos mínimos exigidos
        - Rol y Funciones específicas
        - Modalidad y fecha de inscripción
        - Lugar de realización del Proceso de Selección
        - Datos mínimos a consignar en la Hoja de Vida (o Curriculum Vitae)
        - Prueba de Conocimientos y puntaje mínimo para la aprobación.
    - Publicar la Convocatoria en diario de circulación Provincial.
    - Recibir Hojas de Vida enviadas por los aspirantes en respuesta a la Convocatoria.
- Preselección de aspirantes
    - Analizar y evaluar los datos consignados por los aspirantes en sus respectivas Hojas de Vida y confrontarlos con los
    - requisitos de las vacantes a cubrir.
    - Elaborar Lista de Aspirantes Preseleccionados
- Seleccionar personal

h) Documentación y materiales provistos al personal

Todo el personal involucrado en el funcionamiento de ENCODE S.A. es designado en sus funciones y comunicado de las tareas y procedimientos que debe cumplir.

Del mismo modo, si su función requiere de material adicional, como por ejemplo dispositivos criptográficos, cajas de seguridad, llaves, tarjetas de acceso, etc., éstos son entregados como paso previo a iniciar sus tareas.

A continuación, se detallan las actividades de asignación de recursos al personal de ENCODE S.A.:

Asignación de recursos	Entregar al nuevo empleado la tarjeta de proximidad para acceso al edificio de ENCODE S.A.	RRHH

	Comunicar al nuevo empleado cuál es el puesto de trabajo dentro de ENCODE S.A.	RRHH
	Comunicar al nuevo empleado cuál es la computadora que utilizará para desempeñar sus tareas.	RRHH

Asignación de usuarios y contraseñas	Comunicar al nuevo empleado su identificación de usuario y su contraseña para que pueda llevar a cabo los accesos lógicos correspondientes a su rol y funciones.	Responsable de la Autoridad Certificante ENCODE S.A
Capacitación del personal	Capacitar y entrenar al personal para el puesto de trabajo.	Responsable según corresponda
	Comunicar horarios laborales.	Responsable de RRHH
Asignación de documentación de ENCODE	El personal de ENCODE S.A. es capacitado para poder cumplir con las funciones del rol asociado. Los contenidos básicos se centrarán, entre otros, en los siguientes puntos relevantes:	Responsable de RRHH
	Infraestructura de firma digital.	
	Responsabilidades y compromisos del rol y sus funciones.	
	Procedimientos y políticas operacionales y de seguridad relacionadas con la AR	
	Uso y operaciones de hardware y software empleado.	
	Manejo de incidentes y compromisos en materia de seguridad.	
	Procedimientos de recuperación ante desastres y manejo de la contingencia para la continuidad de actividades.	
	Gestión de la documentación.	

El detalle del material adicional requerido por la Autoridad de Registro figura en el documento “Guía de instalación y funcionamiento de las Autoridades de Registro”.

En el caso de las Autoridades de Registro Delegadas, será responsabilidad de la Organización proveer los elementos adicionales requeridos para desempeñar sus funciones, como paso previo al inicio de las actividades de cada una de ellas.

En conformidad con el material entregado, el personal firma un acuse de recibo y compromiso de confidencialidad en los casos correspondientes.

5.4 Procedimientos de Auditoría de Seguridad

La Autoridad Certificante ENCODE S.A mantiene registros de auditoría (“logs”) de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros y conservándolos por DIEZ (10) años como mínimo. Lo mismo hacen las Autoridades de Registro, dentro de los alcances de sus acciones.

Estos registros de auditoría son utilizados para las tareas de monitoreo habitual del funcionamiento de los sistemas y procesos, para posibles auditorías internas y para las auditorías a que se encuentra sujeto según lo dispuesto en la Ley
N° 25.506 y sus modificatorias.

Los registros de auditoría son analizados por el servicio de monitoreo en las tareas de monitoreo habitual del funcionamiento de los sistemas, las aplicaciones y los procesos.

Con el propósito de mantener la seguridad de los sistemas, el Responsable de Seguridad Informática realiza evaluaciones periódicas sobre los informes servicio de monitoreo, servicio que registra en forma automática las alteraciones en el funcionamiento de la instalación

La información relacionada al registro de eventos se encuentra centralizada en el servidor de monitoreo y es administrado con el software de gestión de eventos.

Este se encargará de recopilar todos los eventos de seguridad, aplicación, sistema y firewalls de los equipos que conforman la plataforma tecnológica de ENCODE S.A.

Estos eventos son monitoreados diariamente por el Responsable de Monitoreo.

El software de gestión de eventos se encuentra configurado para realizar notificaciones en casos de alertas por correo electrónico al Responsable de Monitoreo y al Responsable de Seguridad Informática.

Los registros no electrónicos de acceso físico por parte de solicitantes, suscriptores o terceros son registrados manualmente en el libro de registros de ingresos de la AC de ENCODE S.A., AR Central, ARs Delegadas y Sitio de Contingencia.

5.5 Conservación de registros de eventos

El Certificador genera, mantiene y conserva registros de eventos sobre cada una de las siguientes actividades que comprenden los componentes del proceso de certificación.

La información registrada abarca:

Fecha y hora del registro

Número de serie o secuencia del registro Tipo

de registro

Fuente del registro

Identificación de la entidad que efectuó el registro

Administración del ciclo de vida de las claves criptográficas	1) Generación y almacenamiento de las claves criptográficas del certificador 2) Resguardo y recuperación de las claves criptográficas del certificador 3) Utilización de las claves criptográficas del certificador 4) Archivo de las claves criptográficas del certificador 5) Retiro de servicio de datos relacionados con las claves criptográficas 6) Destrucción de claves criptográficas del certificador 7) Identificación de la entidad que autoriza una operación de administración de claves criptográficas 8) Identificación de la entidad que administra los datos relativos a las claves criptográficas i) Compromiso de la clave privada
Administración del ciclo de vida de los certificados	a) Recepción de solicitudes de certificados nueva o renovación b) Transferencia de claves públicas para la emisión del certificado c) Cambios en los datos de la solicitud del certificado d) Generación de certificados e) Distribución de la clave pública del certificador f) Solicitudes de revocación de certificados g) Generación y emisión de listas de certificados revocados h) Acciones tomadas en relación con la expiración de un certificado

Administración del ciclo de vida de los dispositivos criptográficos	a) Esta actividad estará bajo la responsabilidad del suscriptor y de los oficiales de registro. b) El certificador registra el número de serie del dispositivo que se entrega y quien lo recibe. c) El responsable técnico registra la inicialización del dispositivo criptográfico.
Información relacionada con la solicitud de Certificados	a) Tipos de documentos de identificación presentados por el solicitante b) Otra información de identificación c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación
	d) Identificación de la entidad que recibe y acepta la solicitud e) Método utilizado para validar los documentos de identificación f) Identificación de la Autoridad de Registro
Eventos de seguridad	a) Lecturas y/o escrituras en archivos sensibles de seguridad b) Borrado de datos sensibles de seguridad c) Cambios en los perfiles de seguridad d) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos e) Caídas del sistema, fallas en el hardware y software, u otras anomalías f) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad g) Cambios en la relación entre ENCODE S. A. y una Autoridad de Registro Delegada o personal relacionado con el proceso de certificación h) Accesos a los componentes del sistema de la Autoridad Certificante ENCODE S.A i) i) Eventos o situaciones no previstas

La información relacionada al registro de eventos se encuentra centralizada en el servidor de monitoreo y es administrado con el software de gestión de eventos.

Este se encargará de recopilar todos los eventos de seguridad, aplicación, sistema y firewalls de los equipos que conforman la plataforma tecnológica de ENCODE S.A. Estos eventos son monitoreado diariamente por el Responsable de Monitoreo.
El software de gestión de eventos se encuentra configurado para realizar notificaciones en casos de alertas por correo electrónico al Responsable de Monitoreo y al Responsable de Seguridad Informática.

Los registros no electrónicos de acceso físico por parte de solicitantes, suscriptores o terceros son registrados manualmente en el libro de registros de ingresos de la AC de ENCODE S.A., AR Central, ARs Delegadas y Sitio de Contingencia.

El Responsable de Firma Digital registra:

- En los Libros de Actas de la AC las tareas de resguardo.

- En el Libro de Actas de Contingencia la ceremonia inicial, los controles periódicos, etc. la fecha y un breve resumen de las tareas realizadas y ingreso al Sitio de Máxima Seguridad de Contingencia a las personas no incluidas en la Lista de Contactos Primarios y Sustitutos para la Contingencia (que deben ingresar a este Sitio), el tipo de evento, la fecha y un breve resumen del Inventario de Bienes y Servicios realizado.

El Responsable de la AR registra:

- ✓ En el Libro de Actas de las Autoridades de Registro toda actividad de Revocación de Certificados Digitales.
- ✓ El libro de actas de la Autoridad Certificante se encuentra resguardado en el cofre de seguridad ubicado en el sitio de máxima seguridad de ENCODE S.A.
- ✓ El libro de actas del sitio de contingencia se encuentra resguardado en el cofre de seguridad ubicado en el sitio de máxima seguridad de contingencia.

5.6 Cambio de claves criptográficas

Las claves criptográficas de la Autoridad Certificante ENCODE S.A son generadas con motivo del licenciamiento de la presente Política Única de Certificación de ENCODE S.A. y tendrán una duración de DIEZ (10) años. Por su parte la licencia, en sí misma, tiene una vigencia limitada CINCO (5) de años.

El cambio del par de claves criptográficas de la Autoridad Certificante 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.

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

5.7 Plan de respuesta a incidentes y recuperación ante desastres.

El Plan de Contingencia de ENCODE S.A. como Certificador Licenciado establece los procedimientos y actividades relacionados con el servicio de certificación de firma digital y será de aplicación desde el momento de la declaración de la emergencia hasta la restauración de la operatoria normal.

- **Frecuencia, oportunidad y urgencia**

Un año antes del vencimiento del certificado. Urgencia Alta.

- **Roles que participan en el procedimiento**

a) Responsable de Firma Digital

b) Responsable de la Autoridad Certificante

c) Responsable Técnico

- **Acción que pone en marcha el procedimiento**

Al certificado de la Autoridad Certificante solo le queda un año de vigencia.

- **Tareas a realizar por cada uno de los roles que actúan**

a) El Responsable Técnico inicia el servicio de emisión de Certificados

b) El Responsable Técnico solicita la renovación de certificado de la AC con generación de nuevo par de claves.

c) El Servicio de Emisión de Certificados genera un nuevo requerimiento de solicitud de certificado.

d) El Responsable Técnico copia el requerimiento asociado al nuevo par de claves generadas y lo copia en pendrive

e) El Responsable Técnico entrega el pendrive con el nuevo requerimiento al Responsable de Firma digital

f) El responsable de Firma Digital envía el requerimiento a la Autoridad de Aplicación

g) La Autoridad de Aplicación envía el nuevo certificado

h) El responsable de la Autoridad Certificante autoriza la instalación

i) El Responsable Técnico completa el proceso de instalación del nuevo certificado

j) El responsable de Firma Digital registra en el libro de actas las tareas realizadas.

- **Resultado del procedimiento**

Certificado de Autoridad Certificante Renovado Registro en libro de Actas de renovación de certificado.

5.8 Plan de Cese de Actividades

El Plan de Cese de Actividades de ENCODE S.A., contempla las estrategias y procedimientos a seguir desde la decisión de suspender en forma definitiva el servicio de certificación hasta la inhabilitación lógica y física de la Autoridad Certificante ENCODE S.A. Más información se encuentra en el documento “Plan de Cese de Actividades”.

6. CONTROLES DE SEGURIDAD TÉCNICA

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

Según lo establecido en “6.1.1. Generación del par de claves criptográficas” de la Política Única de Certificación de ENCODE S.A.

6.1.2. Entrega de la clave privada

Según lo establecido en “6.1.2. Entrega de la clave privada” de la Política Única de Certificación de ENCODE S.A.

6.1.3. Entrega de la clave pública al emisor del certificado

Según lo establecido en “6.1.3. Entrega de la clave pública al emisor del certificado” de la Política Única de Certificación de ENCODE S.A.

6.1.4. Disponibilidad de la clave pública del certificador

Según lo establecido en “6.1.4. Disponibilidad de la clave pública del certificador” de la Política Única de Certificación de ENCODE S.A.

6.1.5. Tamaño de claves

Según lo establecido en “6.1.5. Tamaño de claves” de la Política Única de Certificación de ENCODE S.A.

6.1.6. Generación de parámetros de claves asimétricas

Según lo establecido en “6.1.6. Generación de parámetros de claves asimétricas” de la Política Única de Certificación de ENCODE S.A.

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

Según lo establecido en “6.1.7. Propósitos de utilización de claves (campo “KeyUsage” en

certificados X.509 v.3)” de la Política Única de Certificación de ENCODE S.A.

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, las Autoridades de Registro y los suscriptores, según se detalla a continuación.

6.2.1. Controles y Estándares para dispositivos criptográficos

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

Las claves privadas de las Autoridades de Registro son generadas y almacenadas en 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 su elección,

1) por “software”.
2) por “hardware” sobre dispositivos criptográficos diseñados para tal fin que cumplen con las normas FIPS 140-2 nivel 2 validados por ENCODE S.A..
3) “Servicio de firma digital con custodia centralizada de claves criptográficos”, que deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado (como también se deberá cumplir con el uso de dispositivo criptográfico FIPS 140-2 nivel 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 es generada y almacenada por:

1) “software” en el disco de su computador.
2) “sobre dispositivos criptográficos” diseñados para tal fin que cumplen con las normas FIPS 140-2 nivel 2.
3) “Servicio de firma digital con custodia centralizada de claves criptográficos”, que deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado (como también se deberá cumplir con el uso de dispositivo criptográfico FIPS 140-2 nivel 3), cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.

En caso de elección por software las claves deben ser resguardadas con un pin de

seguridad para su acceso. 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 dispositivos validados por ENCODE S.A.

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, dentro del nivel de seguridad asignado a las operaciones críticas de la Autoridad Certificante. Para su activación deben estar presentes, por lo menos, el responsable técnico, el Oficial de seguridad informática y los Oficiales habilitadores o testigos en un número TRES (3) de DIEZ
(10) posibles.

Las Autoridades de Registro y los suscriptores de certificados con dispositivos criptográficos de su propiedad tienen acceso a su clave privada personal a través de un PIN de acceso al dispositivo criptográfico y contraseña de la clave privada.

6.2.3. Recuperación de clave privada

La especificación conceptual puede encontrarse en “6.2.3. Recuperación de clave privada” de la Política Única de Certificación de ENCODE S.A.

Para el procedimiento de recuperación de la clave privada de la Autoridad Certificante ENCODE S.A se debe disponer de la copia de seguridad (“backup”) en un dispositivo HSM de backup. Se debe tener presente que tanto la obtención de la copia como la recuperación sólo pueden ser realizadas 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 ENCODE S.A en su sitio principal o en su sitio alternativo de contingencia.

El procedimiento en sí mismo es reservado, no es información de divulgación pública.

El resultado del procedimiento es la disponibilidad del servicio de certificación digital, en el sitio principal o en el de contingencia, según como se hubiera requerido.

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 a la 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 son realizadas inmediatamente después de su generación por personal autorizado y almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3. Estos dispositivos son resguardos en lugar de acceso restringido.

El procedimiento es reservado.

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

6.2.5. Archivo de clave privada

Las copias de resguardo de la clave privada de la Autoridad Certificante 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.

El procedimiento es reservado.

No se implementan mecanismos de archivo de copias de resguardo de la clave privada de la Autoridad de Registro y de los suscriptores.

6.2.6. Transferencia de claves privadas en dispositivos criptográficos

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

El procedimiento para la Autoridad Certificante ENCODE S.A es reservado.

Las claves privadas de los Oficiales de Registro son generadas y almacenadas por software o en dispositivos criptográficos homologados FIPS 140-2 nivel 2 los que no permiten su exportación.

El procedimiento para los Oficiales de Registro es similar al de los suscriptores, descripto en “4.1. Solicitud de Certificados” para la primera emisión y en las sucesivas renovaciones.

Las claves privadas de los Suscriptores que tengan dispositivos criptográficos son generadas y almacenadas en esos dispositivos, que estarán validadas como FIPS 140-2 nivel 2 y no permiten su exportación. En caso de no poseer dichos dispositivos se implementa por “software”.

El procedimiento para los Suscriptores, descripto en “4.1. Solicitud de Certificados” para la primera emisión y en para las sucesivas renovaciones.

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 ENCODE S.A deben estar presentes, por lo menos, el Responsable Técnico, el Oficial de seguridad informática y los Oficiales habilitadores en número TRES (3) de DIEZ (10). Los responsables necesarios para la activación deberán identificarse frente al sistema según corresponda al rol asignado por medio de distintos mecanismos de autenticación, a saber: llave de seguridad, claves secretas o ambos.

El procedimiento es reservado.

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

6.2.9. Método de desactivación de claves privadas

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

El procedimiento es reservado.

6.2.10. Método de destrucción de claves privadas

Una vez finalizada la vida útil de la clave privada de la Autoridad Certificante ENCODE S.A, con motivo de la revocación o expiración del certificado asociado, la partición del dispositivo criptográfico contenedor de esa clave privada será borrada y “formateada” según el documento Plan de Seguridad.

El procedimiento es reservado.

Para el caso de que finalice la vida útil de la clave privada de una Autoridad de Registro o de un suscriptor, por motivo de revocación o expiración del certificado asociado, y sin mediar renovación, el correspondiente dispositivo criptográfico será inicializado nuevamente por su propietario.

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 las Autoridades de Registro, como así también el de la Autoridad Certificante ENCODE S.A, son almacenados y publicados bajo un esquema de redundancia y respaldados en forma periódica, lo cual, sumado a la firma de ellos, garantiza su integridad.

Todos los certificados son almacenados en soporte magnético, en formato estándar bajo codificación internacional DER. No se requieren herramientas particulares para el tratamiento de dicha información.

El procedimiento para la toma de la copia de respaldo y para su restauración se ejecuta en forma periódica, de acuerdo con un programa establecido. Es requisito previo la disponibilidad de los medios de almacenamiento seguro para contener las copias.

El detalle del procedimiento no es de disponibilidad pública, sino reservada.

6.3.2. Periodo de uso de clave pública y privada

El par de claves criptográficas del certificado de la AUTORIDAD CERTIFICANTE ENCODE S.A tiene una validez de DIEZ (10) años.

El par de claves criptográficas correspondientes a los certificados emitidos por la Autoridad Certificante ENCODE S.A podrán ser utilizadas por su suscriptor únicamente durante el periodo de validez de los certificados. Ese período tiene una validez de DOS (2) años para todos los certificados de persona humana o jurídica.

6.4 Datos de activación

6.4.1. Generación e instalación de datos de activación

Los dispositivos criptográficos utilizados por la Autoridad de Registro Central y los suscriptores que los tengan para la generación, almacenamiento y uso de la clave privada, son inicializados por ellos.

Como paso previo a la generación de la clave privada, los Oficiales de Registro y los suscriptores que posean estos dispositivos, deberán establecer una clave de seguridad de acceso sobre el dispositivo criptográfico denominado PIN, y al momento de la generación, la contraseña de la clave privada. El PIN de acceso del dispositivo criptográfico y 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 ENCODE S.A.

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

Este procedimiento es reservado.

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 del PIN de acceso del dispositivo criptográfico y de la contraseña de la clave privada.

Ni ENCODE S.A., ni la AR Central, ni las AR Delegadas implementan mecanismos de respaldo de las contraseñas de la clave privada ni del PIN de acceso del dispositivo criptográfico de Oficiales de Registro y suscriptores.

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

Este procedimiento es reservado.

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 PIN 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.

El PIN 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

Para la prestación de sus servicios, la Autoridad Certificante ENCODE S.A utiliza una infraestructura tecnológica propia que cumple con los requisitos técnicos establecidos por la normativa vigente.

Entre los controles técnicos utilizados pueden mencionarse:

a) Control de Acceso físicos y lógicos

El acceso físico a las instalaciones está conformado por diversos perímetros de seguridad internos unos de otros, cada uno de los cuales cuenta con mecanismos de tarjeta de proximidad y/o biométricos.

Del mismo modo, el acceso lógico a los sistemas se realiza por medio de servidores "firewall" y sus propios mecanismos de control y monitoreo.

b) Separación de funciones y roles críticos

Las principales funciones vinculadas a los procesos de seguridad y certificación se encuentran divididos en roles que aseguran el correcto desempeño de los responsables designados.

Los roles definidos en la operatoria de la Autoridad Certificante ENCODE S.A serán desempeñados por diferentes responsables. En caso de ausencia temporaria, el responsable será reemplazado por su correspondiente sustituto.

Esto aplica también a la Autoridad de Registro Central y Delegada. Para mayor detalle ver el documento "Guía de instalación y funcionamiento de las Autoridades de Registro".

c) Identificación y autenticación de roles

Para la identificación y autenticación en cada uno de los roles con acceso al Sitio de Máxima Seguridad de ENCODE SA:

- Responsable de la AC
- Responsable Técnico.
- Responsable de Seguridad Informática.
- Responsable de Firma Digital Responsable de SMS.
- Oficial de Seguridad Informática.
- Los cuales se encuentran vinculados al proceso de certificación y gestión de claves de ENCODE S.A. Se utilizan mecanismos de reconocimiento biométrico y sistemas de autenticación de múltiples factores.

d) Utilización de criptografía para las sesiones de comunicación.

Todas las comunicaciones críticas entre los distintos componentes de la Autoridad Certificante ENCODE S.A se realizan en forma cifrada.

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

Se realizan auditorías y controles periódicos sobre cada etapa del proceso de certificación, incluyendo la verificación de la documentación de respaldo del proceso de identificación de suscriptores.

f) Registro de eventos de seguridad. Todas las operaciones y actividades de ENCODE

S.A. generan información de control y registros de eventos que permiten verificar el funcionamiento y la seguridad de los sistemas.

g) Prueba de seguridad.

Se realizan comprobaciones periódicas del funcionamiento de los sistemas y los planes de contingencia.

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

Existen mecanismos y procedimientos de contingencia que garantizan la continuidad en la prestación de los servicios.

6.5.2. Requisitos de seguridad computacional

Los servidores que conforman la Autoridad Certificante ENCODE S.A se encuentran alojados en el "Sitio de Máxima Seguridad" o SMS construido con las certificaciones requeridas 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

Aplicación PKI AC ENCODEDOC

El software PKI utilizado por la AUTORIDAD CERTIFICANTE ENCODE S.A, se basa en todos los servicios de certificados nativos del Microsoft Windows Server, permitiendo a su vez darle soporte documental a todos los circuitos diseñados para implementar la infraestructura de clave pública. Es un software totalmente escalable, modular e integrable, e incluye todas las llamadas a las funciones de Microsoft Windows Server que cuenta con un completo sistema de seguridad diseñado según las normativas de seguridad ITU: X.509v3, RSA: PKCS 1, 7, 9, 10,12 y IETF: RFC2459, CMC.

6.6 Controles Técnicos del ciclo de vida de los sistemas

6.6.1. Controles de desarrollo de sistemas

Los sistemas informáticos adquiridos 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.

El modelo elaborado por la organización OWASP se maneja con una lista de las DIEZ (10) vulnerabilidades más frecuentes encontradas en las aplicaciones web, ordenadas según el número de casos. Esa lista es dinámica y se actualiza con una frecuencia anual para adaptarla a la realidad encontrada mediante encuestas y procesamiento estadístico. Este modelo incluye también la recomendación de procedimientos para detección de cada una de esas vulnerabilidades en las aplicaciones, tanto adquiridas en forma de paquete terminado como en las desarrolladas por la organización.

Más información puede encontrarse en: https://www.owasp.org/

El responsable de aplicaciones de ENCODE S.A. sigue los lineamientos de este modelo, con un grupo de profesionales entrenados. Su misión es certificar el cumplimiento del modelo por parte de cada aplicación antes de su implementación para el servicio de firma digital.

6.6.2. Controles de Gestión de seguridad

ENCODE S.A. mantiene el control de los equipos por medio del inventario y de la documentación de la configuración del sistema, registrándose de inmediato toda modificación o actualización a cualquiera de ellos. Los controles son auditados en forma periódica según las especificaciones de la Política de Seguridad.

El esquema de seguridad física del Sitio de Máxima Seguridad donde se aloja la Autoridad Certificante 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 ENCODE S.A, realizado por el servicio ENCODEMON, advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

6.6.3. Calificaciones de seguridad del ciclo de vida del software

No existen certificaciones de terceros respecto del ciclo de vida del software.

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 ENCODE S.A se encuentra delimitada por 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 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.

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 MM 399 E/2016.

Las listas de certificados revocados (CRLs) cumplen con los requerimientos de la Resolución MM N° 399 E/2016 y las especificaciones contenidas en el RFC 5280.

7.1 Perfil del certificado

El formato de los certificados digitales emitidos bajo esta política cumple con los requerimientos de las Resolución 399 E/2016 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 la Política Única de Certificación se emitirán 4 tipos de certificados:

- Persona humana
- Persona Jurídica
- Sitio seguro

- Aplicación

La información detallada se encuentra en el punto “7.1. Perfil del certificado” de la Política Única de Certificación de ENCODE S.A.

7.2 Perfil de la lista de certificados revocados

La información detallada se encuentra en “7.2. Perfil de la lista de certificados revocados” de la Política Única de Certificación de ENCODE S.A.

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

La información detallada se encuentra en “7.3. Perfil de la la consulta en línea del estado del certificado” de la Política Única de Certificación de ENCODE S.A.

8 . AUDITORIAS DE CUMPLIMIENTO Y OTRAS EVALUACIONES

ENCODE S.A., en su carácter de certificador licenciado, se encuentra sujeto a las auditorias dispuestas en art.34 de la Ley 25.506 y sus modificatorias.

Esas auditorías tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener la condición de Certificador Licenciado y la aplicación de las políticas y procedimientos aprobados por la Autoridad de Aplicación para la Política Única de Certificación de ENCODE S.A.

Los temas principales a evaluar en dichas auditorías son: a)

Requisitos legales generales.

b) Política Única de Certificación de ENCODE S.A. y Manual de Procedimientos de Certificación.

c) Plan de Seguridad.

d) Plan de Cese de Actividades.

e) Plan de Contingencia.

f) Plataforma Tecnológica.

g) Ciclo de vida de las claves criptográficas del certificador.

h) Ciclo de vida de los certificados de suscriptores.

i) Estructura y contenido de los certificados y CRLs.

j) Mecanismos de acceso a la documentación publicada, certificados y CRLs.

k) Pautas para la Autoridad de Registro.

Por su parte, ENCODE S.A. realizará con su Oficial de Auditoría de las Autoridades de Registro, auditorías periódicas a su Autoridad de Registro Central y a sus Autoridades de

Registro habilitadas, para verificar el cumplimiento de los requisitos de su habilitación, siendo los temas principales a evaluar:

a) 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.

b) Las políticas y procedimientos aprobados por la Autoridad de Aplicación para la Política Única de Certificación de ENCODE S.A.

c) En caso de producirse observaciones en las auditorías realizadas, luego de haber sido debidamente notificadas a la autoridad de registro auditada. ENCODE S.A. tomará las medidas correctivas de carácter legal y técnico que amerite el caso. Estas pueden ser desde la supervisión del plan de acción confeccionado por la AR auditada para resolver las no conformidades hasta la aplicación de sanciones a la AR auditada. Los resultados de las auditorías realizadas son presentados por el Oficial de Auditoria al Responsable de Auditoría Interna el cual evaluará los informes obtenidos y los elevará al Directorio de ENCODE.

En cumplimiento del artículo 21 Inciso K de la Ley Nº 25.506, la información relevante de los informes de la última auditoría realizada por la Autoridad de Aplicación, es publicada en los sitios mencionados en "2.2. Publicación de información del certificador" en la Política Única de Certificación de ENCODE S.A.

A continuación, por su relevancia, se describe el procedimiento de Auditoría Interna a las ARs delegadas:

Procedimiento de Auditoría Interna a las ARs Delegadas

➢ Frecuencia, oportunidad y urgencia

Se realizará una auditoría con periodicidad anual a partir de la fecha de la última auditoría. Planificado. Sin fecha fija. Urgencia baja, salvo situación excepcional.

➢ Roles que participan en el procedimiento

a) Responsable de Auditoría Interna de ENCODE S.A.

b) Responsable de Firma Digital de ENCODE S.A.

c) Responsable de la AR Central

d) Responsable de la AR Delegada

e) Oficial de Registro

f) Oficial de Auditoría de las Autoridades de Registro

➢ Acción que pone en marcha el procedimiento

Decisión tomada por la AR Central de ENCODE S.A., de realizar una auditoría interna a la AR Delegada seleccionada.

Haber transcurrido un año desde la última auditoría.

Tareas a realizar por cada uno de los roles que actúan

a) El Responsable de Auditoría Interna llevará a cabo las visitas necesarias a los roles a auditar.

b) El Responsable de Auditoría Interna elaborará un informe de auditoría y lo entregará a los roles auditados, con copia al Responsable de la AR.

c) Los roles auditados corregirán o modificarán lo necesario, de acuerdo a las observaciones del informe de Auditoría Interna.

d) Los roles auditados responderán a Auditoría Interna mediante un informe, con copia al Responsable de la AR Central y al Responsable de Firma Digital.

e) El Responsable de la AR Central evaluará, junto con el Responsable de Firma Digital, el informe de auditoría y la respuesta de los roles auditados.

f) Se definirá el plan de acción de las no conformidades y luego de su presentación y autorización se ejecutará.

g) En caso de corresponder, el Responsable de Firma Digital aplicará las sanciones necesarias, de acuerdo con lo establecido en el punto “5.3. Controles de seguridad del personal” de este Manual de Procedimientos.

➢ Resultado del procedimiento

- Informe de Auditoría Interna.
- Respuesta al Informe por parte de los roles auditados.
- Plan de acción de no conformidades.
- En caso de corresponder, sanciones aplicadas.

9 ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1 Aranceles

Los aranceles se aplicarán según lo indicado en el punto “9.1. – Aranceles” de la Política Única de Certificación de ENCODE S.A.

➢ Frecuencia, oportunidad y urgencia

Disponibilidad permanente. Numerosas veces por día. Planificado. Urgencia alta.

➢ Roles que participan en el procedimiento

I) Solicitante o suscriptor.

II) Oficial de Registro.

➢ Acción que pone en marcha el procedimiento

Presentación del Solicitante o Suscriptor ante la AR Central o la AR Delegada para acreditar fehacientemente su identidad.

➢ Tareas a realizar por cada uno de los roles que actúan

- El solicitante se presenta ante el Oficial de Registro para su identificación.
- El Oficial de Registro verifica la existencia del comprobante de pago de la solicitud y la aplicación de los aranceles correspondientes.

➢ Resultado del procedimiento

Pago de solicitud de certificado verificado.

9.2 Responsabilidad Financiera

La responsabilidad financiera se describe en “9.2. – Responsabilidad Financiera” de la Política Única de Certificación de ENCODE S.A.

9.3 Confidencialidad

Según lo descripto en “9.3. Confidencialidad” de la Política Única de Certificación de ENCODE S.A.

9.3.1.- Información confidencial

Según lo descripto en “9.3.1 Información confidencial” de la Política Única de Certificación de ENCODE S.A.

9.3.2.- Información no confidencial

Según lo descripto en “9.3.2. Información no confidencial” de la Política Única de Certificación de ENCODE S.A.

9.3.3.- Responsabilidades de los roles involucrados

Según lo descripto en “9.3.3. Responsabilidades de los roles involucrados” de la Política Única de Certificación de ENCODE S.A.

9.4 Privacidad

Según lo descripto en “9.4. Privacidad” de la Política Única de Certificación de ENCODE S.A.

9.5 Derechos de Propiedad Intelectual

ENCODE S. A. es propietaria exclusiva de todos los derechos de propiedad intelectual de la Política Única de Certificación de ENCODE S.A., acuerdos, declaraciones, procedimientos y documentos auxiliares referidos a la Autoridad Certificante, 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 Política Única de Certificación de ENCODE S.A., 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

Según lo descripto en “9.6. Responsabilidades y garantías” de la Política Única de

Certificación de ENCODE S.A.

9.7 Deslinde de responsabilidad

Según lo descripto en “9.7. Deslinde de responsabilidad” de la Política Única de Certificación de ENCODE S.A.

9.8 Limitaciones a la responsabilidad frente a terceros

Según lo descripto en “9.8. Limitaciones a la responsabilidad frente a terceros” de la Política

Única de Certificación de ENCODE S.A.

9.9 Compensaciones por daños y perjuicios

No es aplicable.

9.10 Condiciones de vigencia

Según lo descripto en “9.10. Condiciones de vigencia” de la Política Única de Certificación de ENCODE S.A.

9.11 Avisos personales y comunicaciones con los participantes

No aplicable.

9.12 Gestión del ciclo de vida del documento

La Política Única de Certificación de ENCODE S.A. y sus documentos relacionados 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.

9.12.1. Procedimientos de cambio

La Política Única de Certificación de ENCODE S.A. y sus documentos relacionados 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. Esos cambios no serán de magnitud tal

que pueda afectar a los certificados vigentes y su posibilidad de uso para la que fue emitido.

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.

El Responsable de Firma Digital eleva las propuestas al Directorio de ENCODE S.A. sobre los cambios en las Políticas de Certificación, Manuales de Procedimientos y otros documentos de la AUTORIDAD CERTIFICANTE ENCODE S.A.

El Directorio evalúa la viabilidad de los cambios a fin de ser aprobados por el Ente Licenciante.

Una vez aprobados se realiza la actualización de los documentos con su correspondiente versionado.

El Responsable de Firma Digital notificará en forma fehaciente al Ente Licenciante los cambios propuestos para la documentación.

9.12.2. Mecanismo y plazo 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.encodeac.com.ar/firma-digital

En caso de producirse modificaciones sustanciales a los contenidos de la Política Única de Certificación de ENCODE S.A. o a alguno de los documentos relacionados, 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.

9.12.3. Condiciones de modificación del OID

No aplicable.

9.13 Procedimiento de resolución de conflictos

En caso de surgir cualquier discrepancia o conflicto interpretativo 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 procedimiento administrativo, a su cargo, que se describe a continuación.

➢ Frecuencia, oportunidad y urgencia

Disponibilidad permanente. Esporádico. No planificado. Urgencia alta.

➢ Roles que participan en el procedimiento

a) Responsable de Firma Digital.
b) Responsable de la AR Central.
c) Responsable de la AR Delegada.
d) Oficial de Mesa de Ayuda.
e) Solicitante, Suscriptor o Tercero Usuario, que reclama.

➢ Acción que pone en marcha el procedimiento

Presentación del reclamo ante ENCODE S.A., con motivo de la controversia o conflicto.

➢ Tareas a realizar por cada uno de los roles que actúan

a) La persona humana o jurídica realizará su reclamo mediante correo electrónico dirigido a mda@encodesa.com.ar
b) El Sistema de Mesa de Ayuda generará un ticket indicando número de reclamo y rol/persona de ENCODE a la que fue asignada la resolución del reclamo.
c) El Suscriptor reclamante recibirá un correo notificándole el número asignado.
d) Una vez recibida la descripción del conflicto y constatada la divergencia la persona asignada lo resolverá y le comunicará al reclamante la solución encontrada. Si el reclamante está de acuerdo con la misma cerrara el ticket.
e) En caso contrario, la persona asignada al ticket de reclamo lo elevará al Responsable de la AR Central o AR Delegada, quien labrará un acta que deje expresa constancia de los hechos que la motivan y de todas y cada uno de los hechos y antecedentes que le sirvan de causa.
f) Dará traslado del acta, mediante notificación fehaciente, a las partes

involucradas: Oficial de Mesa de Ayuda y/o Solicitante y/o Suscriptor y/o Tercer 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.

g) Finalmente, el Responsable de Firma Digital de 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.

- **Resultado del procedimiento**

Respuesta de ENCODE S.A. a la parte que había presentado el reclamo. Descripción de los hechos en el Sistema de Mesa de Ayuda.

Las partes involucradas en el conflicto podrán recurrir ante la Autoridad de Aplicación, previo agotamiento del procedimiento administrativo recién descripto.

9.14 Legislación aplicable

La legislación aplicable está indicada en “9.14. Legislación aplicable” de la Política Única de Certificación de ENCODE S.A.

9.15 Conformidad con normas aplicables

A los fines de la interpretación y aplicación del presente documento se debe tener en cuenta la normativa indicada en el punto “9.14. Legislación aplicable” de la Política Única de Certificación de ENCODE S.A.

En caso de reclamos de los solicitantes o suscriptores de certificados digitales relacionados con la prestación de servicios de ENCODE S.A., el solicitante, suscriptor o tercero deberá realizar el correspondiente reclamo ante ENCODE S.A., siguiendo el procedimiento indicado en “9.13 Procedimiento de resolución de conflictos”. 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 Clausulas adicionales

No aplicable.

9.17 Otras cuestiones generales

No 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-2021-32177328-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Miércoles 14 de Abril de 2021

Referencia: Manual de Procedimientos de ENCODE S.A. v1.11

El documento fue importado por el sistema GEDO con un total de 76 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.04.14 08:45:26 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2021.04.14 08:45:27 -03:00