INDRA SISTEMAS

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

PKI Interna de Indra (IDR-PKI)

Código: **IDR-PKI-DPC**

Versión: **0.0.1**

Fecha: **25/05/2017**

Control documental

Documento / Fichero	
Título: **Declaración de Prácticas de Certificación**	Nombre fichero:
Código: **IDR-PKI-DPC**	Soporte lógico:
Fecha: **25/05/2017**	Ubicación física:
Versión: **0.0.1**	

Registro de cambios		
Versión	**Fecha**	**Motivo del cambio**
0.0.1	25/05/2017	Primera versión del documento

Distribución del documento	
Nombre	**Área**

Control del documento			
Preparado	**Revisado**	**Aprobado**	**Aceptado**

RESUMEN DE DERECHOS Y OBLIGACIONES ESTABLECIDOS EN ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Este texto constituye únicamente un extracto de los derechos y obligaciones establecidos en la presente Declaración de Prácticas de Certificación (DPC). Su contenido ha de ser complementado con el resumen que se encontrará en la correspondiente Política de Certificación (PC) aplicable al certificado que se esté solicitando o con el que se esté operando.

Es altamente recomendable la lectura completa de esta DPC, así como de las PC que sean de aplicación, para tener una idea clara de los objetivos, especificaciones, normas, derechos, obligaciones y responsabilidades que rigen la prestación del servicio de certificación.

- ✓ Esta DPC y los documentos relacionados regulan todo el ciclo de vida de los certificados electrónicos desde su solicitud hasta su extinción o revocación, así como las relaciones que se establecen entre el solicitante/titular del certificado, la Autoridad de Certificación y los Terceros Aceptantes. Asimismo recoge tanto los certificados electrónicos regulados por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, como los certificados electrónicos de componentes informáticos (no contemplados en dicha Ley).
- ✓ Tanto la DPC como el resto de documentos relacionados están a disposición de los solicitantes, titulares y usuarios de los certificados en la página web https://pki.indraweb.net/politicas.
- ✓ Las Autoridades de Certificación de la PKI de INDRA emiten diversos tipos de certificados, para los que existen Políticas de Certificación (PC) específicas. En consecuencia, el solicitante de cualquier tipo de certificado ha de conocer esta DPC y la PC que en cada caso le sea de aplicación para poder solicitar y usar de forma correcta el certificado.
- ✓ La custodia de las claves privadas por el titular del certificado es requisito fundamental para la seguridad del sistema. En consecuencia, resulta obligado informar de manera inmediata a la Autoridad de Certificación cuando exista alguna de las causas de revocación/suspensión de la vigencia del certificado establecidas en la DPC. Así, se podrá suspender/revocar el certificado comprometido y evitar su uso ilegítimo por un tercero no autorizado.
- ✓ El titular del certificado deberá comunicar a la Autoridad de Certificación cualquier modificación o variación de los datos que se proporcionaron para la obtención del certificado, tanto si éstos se recogieron o no en el propio certificado.
- ✓ El titular debe hacer un uso apropiado del certificado, y será de su exclusiva responsabilidad la utilización del certificado de forma diferente a la prevista en la DPC y en la PC correspondiente.
- ✓ La persona que pretenda confiar en un certificado es responsable de verificar, utilizando las fuentes de información que se ponen a su disposición, que el certificado y el resto de certificados de la cadena de confianza son válidos y no han caducado o han sido suspendidos o revocados.
- ✓ En esta DPC y en las PC relacionadas se establece la delimitación de responsabilidades de las diferentes partes intervinientes así como las limitaciones de las mismas ante posibles daños y perjuicios.

Para más información, consulte la página web establecida al efecto cuya dirección es https://pki.indraweb.net o póngase en contacto con la Autoridad de Certificación mediante la dirección de correo electrónico pki@indra.es.

Índice

1. INTRODUCCIÓN

1.1. RESUMEN

Este documento recoge la Declaración de Practicas de Certificación (DPC) que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública (en adelante PKI) de INDRA (desde ahora INDRAPKI).

Esta DPC se aplica a todas las Autoridades relacionadas con la jerarquía de la PKI de INDRA, incluyendo Autoridades de Certificación (AC), Autoridades de Registro (si las hubiera), Solicitantes y Titulares de certificados y Terceros Aceptantes, entre otros.

La presente DPC se ha estructurado conforme a lo dispuesto por el grupo de trabajo PKIX del IETF (Internet Engineering Task Force), en su documento de referencia RFC 3647 (aprobado en Noviembre de 2003) *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"*. A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC 3647. Cuando no se haya previsto nada en alguna sección aparecerá la frase "No estipulado". Adicionalmente a los epígrafes establecidos en la RFC 3647, se ha incluido un nuevo capítulo dedicado a la Protección de Datos de Carácter Personal para dar cumplimiento a la legislación española en la materia.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta a los estándares europeos, entre los que cabe destacar los siguientes:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.
- 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements.

Igualmente, se ha considerado como legislación básica aplicable a la materia:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.
- Real Decreto Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

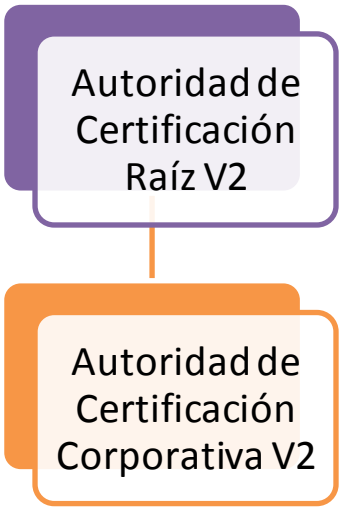
Esta DPC recoge la política de servicios así como la declaración del nivel de garantía ofrecido mediante la descripción de las medidas técnicas y organizativas establecidas para garantizar el nivel de seguridad de la PKI.

La DPC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía de la relación entre INDRAPKI y sus usuarios. En consecuencia, todas las partes involucradas tienen la obligación de conocer la DPC y ajustar su actividad a lo dispuesto en la misma.

La Ley 59/2003, 19 de diciembre, de Firma Electrónica, en su artículo 6 limita la cualidad de titular de los certificados electrónicos a las personas físicas y jurídicas. Ello no obstante, la presente Declaración de Prácticas de Certificación se aplica tanto a los certificados asociados a personas físicas o jurídicas (persona) y por tanto sujetos a la mencionada Ley, como a otra categoría diferente de certificados que son los vinculados a los componentes informáticos, esto es, a los sistemas y servicios corporativos. En función de la categoría de que se trate, certificado de persona o certificado de componente informático, se determina si es o no un certificado electrónico a efectos legales y en consecuencia la aplicabilidad o no de la citada norma.

Esta DPC asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

La arquitectura general, a nivel jerárquico, de la de la PKI de INDRA es la siguiente:



2. ENTIDADES Y PERSONAS INTERVINIENTES

Las Entidades afectadas por esta DPC son:

- INDRA como titular de INDRAPKI.
- Las Autoridades de Certificación.
- Las Autoridades de Registro.
- Los Archivos de Claves.
- Los Solicitantes y Titulares de los certificados emitidos por INDRAPKI.
- Los Terceros Aceptantes de los certificados emitidos por INDRAPKI (si los hubiera).

2.1. AUTORIDADES DE CERTIFICACIÓN

Las Autoridades de Certificación que componen INDRAPKI son:

- "**INDRA AC RAÍZ V2**" como Autoridad de Certificación de primer nivel. Su función es establecer la raíz del modelo de confianza de la PKI. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. Sus datos más relevantes son los siguientes:

Nombre distintivo	CN=INDRA AC RAIZ V2, OU=PKI, O=Indra, C=ES
Huella digital (SHA-1)	71 f8 56 72 1c 01 20 07 3b c9 b7 85 b9 ec 4c 1f 4f 55 b2 25

- "**INDRA AC CORPORATIVA V2**" como Autoridad de Certificación subordinada de "INDRA AC RAÍZ V2". Su función es la emisión de certificados de entidad final de INDRAPKI. Sus datos más relevantes son los siguientes:

Nombre distintivo	CN=INDRA AC CORPORATIVA V2, OU=PKI, O=Indra, C=ES
Huella digital (SHA-1)	fb 96 7c 1d 6c 11 98 06 63 39 b3 17 f8 98 58 ed 00 a4 67 89

2.2. AUTORIDADES DE REGISTRO

Para llevar a cabo la prestación del servicio de Certificación, la AC podrá valerse de una o varias Autoridades de Registro (AR) elegidas libremente. Las Autoridades de Registro (AR) llevarán a cabo la identificación de los Solicitantes de Certificados conforme a las normas de esta DPC y el acuerdo suscrito con la AC. En el caso de que las AR sean de INDRA no será precisa la firma de ningún acuerdo y las relaciones entre ambas se regirán por la presente DPC y las PC que sean de aplicación.

Las Autoridades de Registro competentes para la gestión de solicitudes de certificación se encuentran definidas en la Política de Certificación correspondiente a cada tipo de certificado.

2.3. ARCHIVO DE CLAVES

Las Políticas de Certificación podrán establecer la existencia de un Archivo de Claves para permitir el archivo y recuperación de las claves privadas de los titulares para los certificados que regulen. El Archivo de Claves deberá garantizar la confidencialidad de la clave privada y su recuperación deberá exigir, como mínimo, la intervención de dos personas diferentes. En la PC se deberán regular los procedimientos de petición y tramitación de recuperaciones de claves.

2.4. TITULARES DE LOS CERTIFICADOS

Se denomina Titular de un certificado a toda aquella persona física o jurídica o componente informático a cuyo nombre se emite un certificado en el ámbito de INDRAPKI. La titularidad es efectiva una vez que el certificado es emitido por la AC y aceptado por su solicitante.

Los tipos de entidades que pueden ser titulares de certificados de INDRAPKI se encuentran definidos y limitados por cada Política de Certificación. De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, en la siguiente tabla se pueden observar algunas clases de titulares existentes en INDRAPKI:

Tabla 1 Titulares de los certificados

Entorno de Certificación	Titulares
INDRA AC Corporativa V2	Empleados de Indra Colaboradores de Indra con acceso a los Sistemas de Información de Indra Personal de Empresas Contratadas con acceso a los Sistemas de Información de Indra

Como futuro titular o responsable del componente para el que se pide el certificado, toda persona deberá ajustarse a los procedimientos establecidos para la solicitud de cada tipo de certificado, y cumplir los requisitos que se establezcan en la DPC y en la PC de los diferentes certificados.

Las personas que pueden solicitar la emisión de certificados de INDRAPKI se encuentran definidas y limitadas por cada Política de Certificación.

2.5. TERCEROS ACEPTANTES

Las Políticas de Certificación correspondientes a cada tipo de certificado son quienes determinan los Terceros Aceptantes de cada certificado. No es objetivo de está DPC su determinación.

2.6. OTROS AFECTADOS

Solicitantes: personas físicas, personas jurídicas, a través de sus representantes y componentes informáticos, a través de sus responsables, que han solicitado la emisión de un certificado a INDRAPKI.

3. USO DE LOS CERTIFICADOS

3.1. USOS APROPIADOS DE LOS CERTIFICADOS

Las Políticas de Certificación correspondientes a cada tipo de certificado son quienes determinan los usos apropiados que debe darse a cada certificado. No es objetivo de esta DPC la determinación de dichos usos.

3.2. LIMITACIONES Y RESTRICCIONES EN EL USO DE LOS CERTIFICADOS

Los certificados deben emplearse de acuerdo con las funciones y finalidades definidas en su correspondiente PC, sin que puedan utilizarse para otras tareas y otros fines no contemplados en aquella.

Igualmente, los certificados deben emplearse únicamente de acuerdo con la legislación que le sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados, salvo en los casos en que así lo especifique la PC, no pueden emplearse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

Los servicios de certificación que ofrece INDRAPKI, no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como el funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otras donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

Las Políticas de Certificación correspondientes a cada tipo de certificado pueden determinar limitaciones y restricciones adicionales en el uso de los certificados. No es objetivo de esta DPC la determinación de dichas limitaciones y restricciones adicionales..

3.3. ADMINISTRACIÓN DE LAS POLÍTICAS

3.3.1. Especificación de la Organización Administradora

Esta DPC es propiedad de INDRA:

Nombre	Indra
Dirección e-mail	pki@indra.es
Dirección	Avda. de Bruselas, 35

	Parque Empresarial Arroyo de la Vega 28108 Alcobendas, Madrid (España)		
Teléfono	(+34) 91 480 50 00	**Fax**	(+34) 91 480 50 80

3.3.2. Persona de contacto

Esta DPC está administrada por la Autoridad de Aprobación de Políticas (AAP) de la PKI de INDRA.

Nombre	Autoridad de Aprobación de Políticas (AAP) de la PKI de INDRA		
Dirección e-mail	pki@indra.es		
Dirección	Avda. de Bruselas, 35 Parque Empresarial Arroyo de la Vega 28108 Alcobendas, Madrid (España)		
Teléfono	(+34) 91 480 50 00	**Fax**	(+34) 91 480 50 80

3.3.3. Determinación de la adecuación de la DPC de una AC externa a las Políticas de Certificación de INDRAPKI

En el caso de que se tuviese que evaluar la posibilidad de que una AC interactúe con INDRAPKI la Autoridad de Aprobación de Políticas (AAP) de INDRAPKI es la Autoridad que determina la adecuación de dicha AC a la Política de Certificación afectada. Los procedimientos para determinar la adecuación se recogen en la PC que tenga prevista la posibilidad de operar con otras AC.

3.3.4. Procedimientos de Aprobación de esta PC

La Autoridad de Aprobación de Políticas (AAP) de INDRAPKI es la Autoridad encargada de la aprobación en el momento de su creación de la presente DPC, así como de las Políticas de Certificación (PC).

La AAP también es la competente para aprobar las modificaciones de dichos documentos.

3.4. DEFINICIONES Y ACRÓNIMOS

3.4.1. Definiciones

En el ámbito de esta PC se utilizan las siguientes denominaciones:

Autenticación: procedimiento de comprobación de la identidad de un solicitante o titular de certificados de INDRAPKI.

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Esta es la definición de la Ley 59/2003 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

Directorio: Repositorio de información que sigue el estándar X.500 de ITU-T.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados de INDRAPKI.

Identificador de usuario: conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

Jerarquía de confianza: Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad una o varias de nivel inferior. En el caso de INDRAPKI, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Solicitante: persona que solicita un certificado para sí mismo, para una persona jurídica o para un componente informático.

Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por INDRAPKI.

Titular: persona o componente informático para el que se expide un certificado electrónico y es aceptado por éste o por su solicitante en el caso de los certificados de componente o por el representante en el supuesto de persona jurídica.

3.4.2. Acrónimos

AAP: Autoridad de Aprobación de Políticas

AC: Autoridad de Certificación

AR: Autoridad de Registro

CRL: Certificate Revocation List (Lista de Certificados Revocados)

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CEN: Comité Européen de Normalisation

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CWA: CEN Workshop Agreement

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

DPC: Declaración de Prácticas de Certificación

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard (Estándar USA de procesado de información)

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)

LDAP: Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio)

OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

OID: Object identifier (Identificador de objeto único)

OU: Organizacional Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PC: Política de Certificación

PKCS: Public Key Infrastructure Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

INDRAPKI: PKI de Indra.

RFC: Request For Comments (Estándar emitido por la IETF)

4. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

4.1. REPOSITORIOS

El repositorio de INDRAPKI está compuesto por un servicio de directorio vía Directorio Activo de Microsoft, de uso interno de Indra, y un servicio Web, con acceso libre, que son los siguientes:

Tabla 2 Información del repositorio de INDRAPKI

Clave	Valor
[URL CPS]	https://pki.indraweb.net/politicas
[HTTP URI ROOT CA]	https://pki.indraweb.net/certs/indra-root-v2.crt
[HTTP URI CORP CA]	https://pki.indraweb.net/certs/indra-corp-v2.crt
[AD URI ROOT CA]	ldap:///CN=INDRA%20AC%20RAIZ%20V2,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=indra,DC=es?cACertificate?base?objectdass=certificationAuthority
[AD URI CORP CA]	ldap:///CN=INDRA%20AC%20CORPORATIVA%20V2,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=indra,DC=es?cACertificate?base?objectclass=certificationAuthority
[HTTP URI ARL]	https://pki.indraweb.net/crls/indra-root-v2.crl
[AD URI ARL]	ldap:///CN=INDRA%20AC%20RAIZ%20V2,CN=MADCPVPPKIV2ROOT,CN=CDP,CN=Public%20Key%20Services,CN=Configuration,DC=Indra,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
[HTTP URI CORP CRL]	https://pki.indraweb.net/crls/indra-corp-v2.crl
[AD URI CORP CRL]	ldap:///CN=INDRA%20AC%20CORPORATIVA%20V2,CN=MADCPVPPKIV2CO,CN=CDP, CN=Public%20Key%20Services,CN=Configuration,DC=Indra,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint

Para las DPC y las PC (hasta la fecha de publicación de esta DPC):

- https://pki.indraweb.net/politicas

Desde la página se accede a los siguientes documentos:

- Declaración de Prácticas de Certificación (el presente documento)
- Declaración Básica
- Política de Certificación del certificado de Autenticación
- Política de Certificación del certificado de Firma Electrónica
- Política de Certificación del certificado de Cifrado
- Política de Certificación del certificado de Servidor Seguro SSL

- Política de Certificación del certificado de Controlador de Dominio Windows
- Política de Certificación del certificado de Firma de Código

El repositorio de INDRAPKI no contiene ninguna información de naturaleza confidencial.

4.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Es obligación de las ACs pertenecientes a la jerarquía de confianza de INDRAPKI publicar información relativa a sus prácticas, a sus certificados y el estado actual de dichos certificados.

La presente DPC es pública y se encuentra disponible en el sitio Web de INDRAPKI, al que se hace referencia en el apartado *4.1 REPOSITORIOS*, en formato PDF.

Las Políticas de Certificación de INDRAPKI son públicas y se encuentran disponibles en el sitio Web de INDRAPKI, al que se hace referencia en el apartado *4.1 REPOSITORIOS,* en formato PDF.

Las Listas de Certificados Revocados (CRL) por INDRAPKI son públicas y se encuentran disponibles, en formato CRL v2, en el repositorio y sitio Web de INDRAPKI al que se hace referencia en el apartado *4.1 REPOSITORIOS*. Hasta la puesta en funcionamiento del servicio de validación en línea de INDRAPKI, al expirar el periodo de validez de un Certificado, éste permanecerá incluido en la CRL.

Las Listas de Certificados Revocados irán autenticadas por INDRAPKI mediante firma electrónica de la propia AC.

La información sobre el estado de los certificados se podrá consultar accediendo directamente a las CRL (a fecha de publicación de esta DCP INDRAPKI no dispone de servicio de validación en línea que implementa el protocolo OCSP).

4.3. TEMPORALIDAD O FRECUENCIA DE PUBLICACIÓN

La DPC y las Políticas de Certificación se publicarán en el momento de su creación y se volverán a publicar en el momento en que se apruebe cualquier modificación sobre las mismas. Cuando se realicen modificaciones significativas en la DPC o PC's de INDRAPKI, éstas se notificarán mediante correo electrónico a los titulares de los certificados afectados en el caso de PC's y a los titulares de todos los certificados en el caso de esta DPC. Adicionalmente, las modificaciones se harán públicas en el sitio web referido en el apartado *4.1 REPOSITORIOS*.

Esta notificación se realizará con anterioridad a la entrada en vigor de la modificación que la haya producido.

La AC añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto *6.9.7 Frecuencia de emisión de CRLs.*

4.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la lectura a las DPC y PC es abierto, pero sólo INDRAPKI está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello INDRAPKI establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.

5. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS

5.1. NOMBRES

5.1.1. Tipos de nombres

Todos los titulares de certificados requieren un nombre distintivo (*Distinguished Name*) conforme con el estándar X.500.

Los nombres distintivos vienen dados por la política a tal efecto desarrollada y descrita en el documento de Política de Certificación correspondiente al certificado en cuestión. Esta política debe estar en consonancia con las directrices generales descritas en este capítulo de la DPC.

5.1.2. Necesidad de que los nombres sean significativos

En todos los casos se recomienda que los nombres distintivos de los titulares de los certificados sean significativos.

En cualquier supuesto el dotar a los nombres distintivos de significado viene dado por la política a tal efecto desarrollada y descrita en el documento de Política de Certificación correspondiente al certificado en cuestión.

5.1.3. Reglas para interpretar varios formatos de nombres

La regla utilizada por INDRAPKI para interpretar los nombres distintivos de los titulares de los certificados que emite es ISO/IEC 9595 (X.500) *Distinguished Name* (DN).

5.1.4. Unicidad de los nombres

Los nombres distintivos (*distinguished names*) deben ser únicos y no ambiguos.

Las Políticas de Certificación pueden disponer la sustitución de este procedimiento de unicidad.

5.1.5. Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto *11.13 PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS* de esta DPC.

5.1.6. Reconocimiento, autenticación y papel de las marcas registradas

No estipulado.

5.2. VALIDACIÓN DE LA IDENTIDAD INICIAL

5.2.1. Medio de prueba de posesión de la clave privada

En caso de que el par de claves sea generado por el solicitante del Certificado, éste deberá probar la posesión de la clave privada correspondiente a la clave pública para la que solicita que se genere un certificado, mediante el envío de la solicitud de certificación.

Este procedimiento podrá ser modificado por lo que establezca en cada caso la Política de Certificación aplicable.

5.2.2. Autenticación de la identidad de una organización

En el caso que una Política de Certificación considere necesaria la autenticación de la identidad de una organización por emitirse certificados de persona jurídica o de componente informático, dicha política será la responsable del establecimiento de los métodos necesarios para la verificación de la mencionada identidad

5.2.3. Autenticación de la identidad de una persona física

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

No se considerará que el proceso deba ser menos estricto que otros mecanismos de autenticación utilizados por INDRA.

Como norma general no se emplearán métodos de identificación/autenticación remotos distintos a la firma electrónica realizada con certificados emitidos por la propia INDRAPKI.

En cada PC se establecerá la información a proporcionar por el solicitante, determinándose entre otros aspectos los siguientes:

- Tipos de documentos de identidad válidos para la identificación.
- Cómo la AC o AR autentican al individuo.
- Necesidad o no de identificación presencial.
- Forma de acreditar la pertenencia a una determinada organización.

5.2.4. Información no verificada sobre el solicitante

Cada PC establecerá qué parte de la información suministrada en la solicitud de un certificado no se verifica.

5.2.5. Validación de la autoridad

En los casos en que el certificado se obtenga en nombre de una persona jurídica o un componente informático, la PC deberá establecer cómo se verifican las facultades de representación del solicitante para actuar en nombre de la persona jurídica o del responsable en el caso del componente informático.

5.2.6. Criterios para operar con AC externas

Antes de establecer relaciones de interactividad con AC externas se ha de determinar para ello la adecuación de dichas AC al cumplimiento de ciertos requisitos. Los criterios mínimos que pueden ser ampliados en cada caso por la AAP para considerar a una AC adecuada para interaccionar con INDRAPKI son:

- La AC externa ha de proporcionar un nivel de seguridad en la gestión de los certificados, a lo largo de su ciclo de vida, como mínimo, igual al de la INDRAPKI. Esta exigencia se recogerá en la DPC y PC correspondientes y en su cumplimiento por la AC.
- Ha de cumplir el estándar ETSI TS 101 456: *Policy Requirements for certification authorities issuing qualified certificates* o equivalente.
- Deberá aportar el informe de auditoría de una Autoridad externa de reconocido prestigio relativa a sus operaciones como medio de verificación del nivel de seguridad existente. La AAP podrá declarar exentas de este requisito a las AC pertenecientes a Administraciones Públicas.
- Establecer un convenio de colaboración en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluido en la interacción.

Aunque una AC cumpla los requisitos anteriores la AAP podrá denegar la solicitud de interactividad sin necesidad de aportar ninguna justificación.

La interactividad puede llevarse a cabo mediante certificación cruzada, certificación unilateral u otras formas.

5.3. IDENTIFICACIÓN Y AUTENTICACIÓN EN LAS PETICIONES DE RENOVACIÓN DE CLAVES

5.3.1. Identificación y autenticación por una renovación de claves de rutina

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

Como norma general no se emplearán métodos de identificación/autenticación remotos distintos a la firma electrónica realizada con certificados emitidos por la propia INDRAPKI.

5.3.2. Identificación y autenticación por una renovación de claves tras una revocación

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado, debiendo ser como mínimo tan estricto como el aplicado en la solicitud inicial del certificado.

Como norma general no se emplearán métodos de identificación/autenticación remotos distintos a la firma electrónica realizada con certificados emitidos por la propia INDRAPKI.

6. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

6.1. SOLICITUD DE CERTIFICADOS

6.1.1. Quién puede efectuar una solicitud

La petición para que una persona o componente se convierta en titular de un certificado debe ser realizada por:

- La propia persona, si ya dispone de un certificado de autenticación, **en los casos en que la PC lo permita**.
- Por la persona o departamento autorizado de INDRA con poder para actuar en representación del potencial Titular. Estos "representantes" deberán disponer de un certificado de autenticación y disponer de privilegios de administración de usuarios. En este caso, bien la AR, bien la AC correspondiente serán las encargadas de generar las claves y los certificados de autenticación en lugar de los titulares.
- El proceso de identificación de componentes hardware o software (como un servidor web) se define por la Política de Certificación de Componentes. Como regla general la petición para que un componente se convierta en Titular de un certificado debe ser realizada por el responsable técnico del servicio que gestione dicho componente. La AC o AR deben, además, verificar la identidad del individuo o departamento que realiza la petición y su autoridad para recibir las claves para ese componente.

En cada Política de Certificación se concreta quién puede solicitar un certificado y la información que se debe suministrar en la solicitud. Asimismo, la PC establece los pasos que deben seguirse para llevar a cabo este proceso.

6.1.2. Registro de las solicitudes de certificados y responsabilidades de los solicitantes

En general, es atribución de cada Autoridad de Registro de INDRAPKI determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la Política de Certificación aplicable en cada caso. Ello determinará autorizar o denegar la solicitud de certificación.

Las solicitudes de los certificados, una vez completadas, serán enviadas a la Autoridad de Certificación por la Autoridad de Registro de INDRAPKI.

Como regla general, todo solicitante que desee un certificado tendrá que cumplir los siguientes requisitos:

- Proteger la clave privada de todo compromiso, pérdida, revelación, modificación o uso no autorizado de su clave privada, independientemente del dispositivo de almacenamiento de la misma. Cada solicitante de certificado y, posteriormente a la autorización, cada titular, reconoce que es el responsable de proteger su clave privada y no INDRA.
- Cumplimentar el formulario de solicitud del certificado con toda la información que INDRAPKI requiera para la emisión del mismo. Cabe destacar que no toda la información solicitada aparecerá en el certificado y que ésta será conservada, de manera confidencial, por la

Autoridad de Certificación de acuerdo con la legislación vigente en materia de Protección de Datos Personales.

- Entregar la solicitud de certificado, incluyendo la clave pública, a la AR correspondiente, en el caso de que el certificado tenga su origen en dicha solicitud.
- La existencia de formulario de solicitud y en general el procedimiento de solicitud de certificados a INDRAPKI queda definido en la Política de Certificación correspondiente a cada uno de los certificados.

6.2. TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

6.2.1. Realización de las funciones de identificación y autenticación

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado. No se considerará que el proceso deba ser menos estricto que otros procedimientos de autenticación utilizados por INDRA.

6.2.2. Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que INDRAPKI haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El procedimiento por el que se determina la naturaleza y la forma de realizar dichas comprobaciones se establece en la Política de Certificación correspondiente.

INDRAPKI no es responsable de la idoneidad y exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, éste podrá ser revocado.

Una AC de INDRAPKI puede negarse a emitir un certificado de cualquier solicitante basándose exclusivamente en su propio criterio, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse de tal negativa.

6.2.3. Plazo para la tramitación de las solicitudes de certificados

Las AC de INDRAPKI no se hacen responsables de cualquier demora que pueda surgir en el periodo comprendido entre la solicitud del certificado, la publicación, si procede, y la entrega del mismo. En todo caso se establecerán plazos mínimos para la tramitación de las solicitudes de los certificados en las PC correspondientes.

6.3. EMISIÓN DE CERTIFICADOS

6.3.1. Actuaciones de la AC durante la emisión del certificado

La emisión del certificado implica la autorización definitiva de la solicitud por parte de la AC.

Cuando la AC de INDRAPKI emita un certificado de acuerdo con una solicitud de certificación efectuará las notificaciones que se establecen en el apartado *6.3.2* del presente capítulo.

Todos los certificados iniciarán su vigencia en el momento de su emisión, salvo que se indique en los mismos una fecha y hora posterior a su entrada en vigor, que no será posterior a los 15 días desde su emisión). El periodo de vigencia estará sujeto a una posible extinción anticipada cuando se den las causas que motiven la suspensión o revocación del certificado.

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de certificados acogidos a las mismas.

6.3.2. Notificación al solicitante de la emisión por la AC del certificado

Cada PC establecerá la forma por la que el solicitante haya de conocer la emisión de su certificado La aceptación del certificado es la acción mediante la que su titular da inicio a sus obligaciones respecto a la PKI de INDRA.

6.4. ACEPTACIÓN DEL CERTIFICADO

6.4.1. Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto a la PKI de INDRA.

Los certificados que exijan un registro presencial llevarán aparejada la aceptación explicita del titular del certificado y el reconocimiento de que está de acuerdo en los términos y condiciones contenidos en el contrato que rige los derechos y obligaciones entre INDRAPKI y el titular y de que este conoce la presente Declaración de Prácticas de Certificación, que rige técnica y operativamente los servicios de certificación electrónica prestados por INDRAPKI.

En los casos en que el registro sea telemático, la aceptación de las condiciones se hará de forma electrónica.

En la PC correspondiente se podrán detallar o ampliar la forma en que se acepta el certificado.

6.4.2. Publicación del certificado por la AC

En cada PC se establecerá la publicación del certificado en el repositorio de INDRAPKI.

6.4.3. Notificación de la emisión del certificado por la AC a otras Autoridades

Cuando la AC de INDRAPKI emita un certificado de acuerdo con una solicitud de certificación enviará una copia del mismo a la AR que remitió la solicitud, siempre que ésta fuese tramitada a través de una AR.

6.5. PAR DE CLAVES Y USO DEL CERTIFICADO

6.5.1. Uso de la clave privada y del certificado por el titular

Las responsabilidades y limitaciones de uso del par de claves y del certificado se establecerán en la correspondiente PC. De modo general, los certificados de personas físicas o jurídicas sólo podrán utilizarse mediante dispositivos seguros de creación de firma electrónica.

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en la PC y de forma coherente con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado. Del mismo modo el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones uso, establecidas en la DPC y PC, y sólo para lo que éstas establezcan.

Tras la expiración o revocación del certificado el titular deberá dejar de usar la clave privada.

6.5.2. Uso de la clave pública y del certificado por los terceros aceptantes

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establezca la correspondiente PC y de forma coherente con lo establecido en el campo 'Key Usage' del certificado.

Los Terceros Aceptantes han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC y en la correspondiente PC. Asimismo, se obligan a las condiciones de uso establecidas en dichos documentos.

6.6. RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

6.6.1. Circunstancias para la renovación de certificados sin cambio de claves

Todas las renovaciones de certificados realizadas en el ámbito de esta DPC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de los puntos del apartado 4.6 (4.6.2 a 4.6.7) que establece la RFC 3647, lo que implica, a efectos de esta Declaración, su no estipulación.

6.7. RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

6.7.1. Circunstancias para una renovación con cambio claves de un certificado

El proceso de renovación de certificados dependerá de la Política de Certificación aplicable a cada tipo de certificado.

Un certificado puede ser renovado, entre otros, por los siguientes motivos:

- Expiración del periodo de validez
- Cambio de datos contenidos en el certificado
- Claves comprometidas
- Fiabilidad de claves
- Cambio de formato

Todas las renovaciones de certificados en el ámbito de esta DPC se realizarán con cambio de claves.

6.7.2. Quién puede pedir la renovación de un certificado

Deberá solicitar la renovación el titular del certificado, si bien no todos los certificados prevén el establecimiento de una solicitud de renovación de certificados, quedando establecido en la correspondiente Política de Certificación y prevaleciendo sobre lo estipulado en este apartado de la DPC.

6.7.3. Tramitación de las peticiones de renovación de certificados con cambio de claves

La AC comprobará en el proceso de renovación que la información utilizada para verificar la identidad y atributos del titular es todavía válida. Si alguna información del titular ha cambiado ésta deberá ser verificada y registrada con el acuerdo del titular.

La política de identificación y autenticación para la renovación de un certificado contempla, de forma general, tres casos:

- Renovación por caducidad del certificado siendo la renovación anterior presencial: en este caso la renovación se podrá realizar, si el mecanismo estuviese disponible, de forma remota identificándose mediante un certificado de autenticación de INDRAPKI en vigor.
- Renovación por caducidad del certificado siendo la renovación anterior en línea o renovación por otras causas: en este caso la renovación se solicitará de forma presencial en los puestos de registro que se establezcan de igual forma que en el caso de la emisión inicial.
- Renovación de un certificado de servidor o componente: todas las renovaciones se realizarán de forma remota, efectuando la solicitud mediante correo electrónico firmado con un certificado de firma de INDRAPKI válido.

Estas directrices están supeditadas a la Política de Certificación aplicada a cada certificado, prevaleciendo siempre lo estipulado en la correspondiente política.

Si alguna de las condiciones establecidas en esta DPC o en la PC de aplicación hubieran cambiado se deberá asegurar que tal hecho es conocido por el titular del certificado y que éste está de acuerdo con las mismas.

En cualquier caso la renovación de un certificado está supeditada a:

- Que se solicite en debido tiempo y forma, siguiendo las instrucciones y normas que INDRAPKI especifica a tal efecto.
- Que la AC no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación / suspensión del certificado.
- Que la solicitud de renovación de los servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

6.7.4. Notificación de la emisión de un nuevo certificado al titular

En cada PC se establecerá la forma en que el solicitante conocerá que ha sido emitido el correspondiente certificado a su nombre.

6.7.5. Forma de aceptación del certificado con las claves cambiadas

En cada PC se establecerá la forma en que el solicitante conocerá que ha sido emitido el correspondiente certificado a su nombre.

6.7.6. Publicación del certificado con las nuevas claves por la AC

En cada PC se establecerá la publicación del certificado en el repositorio de INDRAPKI.

6.7.7. Notificación de la emisión del certificado por la AC a otras Autoridades

Cuando la AC de INDRAPKI emita un certificado de acuerdo con una solicitud de certificación enviará una copia del mismo a la AR que remitió la solicitud, siempre que la solicitud de certificado fuera tramitada a través de una AR.

6.8. MODIFICACIÓN DE CERTIFICADOS

6.8.1. Circunstancias para la modificación de un certificado

Se habla de modificación de un certificado cuando se emite uno nuevo debido a cambios en la información del certificado no relacionados con su clave pública o expiración del periodo de validez.

Las modificaciones de los certificados pueden venir dadas por diferentes motivos tales como:

- Cambio de nombre.
- Cambio en las funciones dentro de la organización.
- Reorganización como resultado del cambio en el Nombre Distintitivo.

Todas las modificaciones de certificados realizadas en el ámbito de esta DPC se tratarán como una renovación de certificados, por lo que son de aplicación los apartados anteriores al respecto.

En consecuencia, no se recogen el resto de subapartados del apartado 4.8 (4.8.2 a 4.8.7) que establece la RFC 3647, lo que implica a efectos de esta Declaración que no han sido regulados.

6.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

6.9.1. Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su caducidad. El efecto de la revocación de un certificado es la pérdida de vigencia del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y,

en consecuencia, de la prestación de los servicios de certificación. La revocación de un certificado impide el uso legítimo del mismo por parte del titular.

El proceso de solicitud de revocación se define en la Política de Certificación aplicable a cada tipo de certificado.

La revocación de un certificado implica la publicación de éste certificado en la Lista de Certificados Revocados (CRL) de acceso público.

Causas de revocación:

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales del acuerdo de suscripción, la PC asociada o de la presente DPC.
- El titular de un certificado deja de pertenecer al grupo, circunstancia que le facultaba para la posesión del certificado o bien INDRAPKI cesa en su actividad.
- Emisión defectuosa de un certificado debido a que:
    1. No se ha cumplido un requisito material para la emisión del certificado.
    2. La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
    3. Existencia de un error de entrada de datos u otro error de proceso.
- El par de claves generado por un titular se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud deviene en inexacta.
- Por orden formulada por el firmante.
- Por orden formulada por un tercero autorizado o la persona física solicitante en representación de una persona jurídica.
- El certificado de una AR o AC superior en la jerarquía de confianza del certificado es revocado.
- Por la concurrencia de cualquier otra causa especificada en la presente DPC o en las correspondientes Políticas de Certificación establecidas para cada tipo de Certificado.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez del mismo, deviniendo el certificado como no valido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta DPC ni tendrá efectos retroactivos.

6.9.2. Quien puede solicitar la revocación

INDRAPKI o cualquiera de las Autoridades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del titular, o cualquier otro hecho determinante que recomendara emprender dicha acción. En particular:

- Las Autoridades y Agentes de Registro homologados por INDRA podrán tramitar peticiones de revocación de aquellos certificados, una vez hayan cumplido con el requisito de identificación del solicitante.
- Los titulares de certificados, debiendo solicitar la revocación de acuerdo con las condiciones especificadas en el siguiente apartado 6.9.3.

La política de identificación para las solicitudes de revocación podrá ser la misma que para el registro inicial. La política de autenticación aceptará solicitudes de revocación firmadas electrónicamente por

el titular del certificado, siempre que lo haga con un certificado en vigor diferente del que solicita sea revocado.

Las distintas Políticas de Certificación podrán definir otras políticas de identificación que sean más rigurosas. (p.e. una Política de Certificación pueden definir la creación de una contraseña de revocación en el momento del registro del certificado).

6.9.3. Procedimiento de solicitud de revocación

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.

De forma general y sin perjuicio de lo definido en las Políticas de Certificación se establece que:

- Serán admitidas solicitudes de revocación remotas si están firmadas electrónicamente con un certificado de INDRAPKI y de presencia si se cumplen los requisitos de identificación del usuario establecidos para el registro inicial.
- Se comunicará al titular del certificado la revocación del mismo mediante correo electrónico.
- Tras la revocación del certificado el titular del mismo deberá destruir la clave privada que se corresponda con aquel.
- La revocación de un certificado de autenticación conlleva la revocación del resto de certificados asociados a un titular.

La información a suministrar para solicitar la revocación de un certificado queda a expensas de lo especificado en la correspondiente Política de Certificación.

6.9.4. Periodo de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

6.9.5. Plazo en el que la AC debe resolver la solicitud de revocación

Cada PC establecerá el tiempo máximo para la resolución de una solicitud de revocación, si bien se establece como norma general que se haga en menos de 24 horas.

6.9.6. Requisitos de verificación de las revocaciones por los terceros aceptantes

La verificación de las revocaciones, ya sea mediante consulta directa de la CRL, es obligatoria para cada uso de los certificados por los Terceros Aceptantes.

Los Terceros Aceptantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargar la nueva CRL del repositorio de INDRAPKI al finalizar el periodo de validez de la que posean. Las listas de CRLs guardadas en memoria 'cache', aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Cuando la PC de aplicación soporte otras formas de divulgación de información de revocación, los requisitos para la comprobación de dicha información se especificarán en la propia PC.

6.9.7. Frecuencia de emisión de CRLs

INDRAPKI publicará una nueva CRL en su repositorio en el momento en que se produzca cualquier revocación, y, en último caso, a intervalos no superiores a 24 horas (aunque no se hayan producido modificaciones en la CRL) para las ACs Subordinadas y de 1 año para la AC Raíz.

6.9.8. Tiempo máximo entre la generación y la publicación de las CRL

Cada PC establecerá el tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio.

6.9.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados

INDRAPKI proporciona un servidor web donde publica las CRLs, cuya ubicación queda reflejada en el apartado *4.1 REPOSITORIOS*, para la verificación del estado de los certificados que emite.

Asimismo se prevé la disponibilidad de una Autoridad de Validación que, mediante el protocolo OCSP, permitirá verificar el estado de los certificados. Se comunicará a todos los poseedores de certificados de INDRAPKI el momento exacto en que dicho servicio esté disponible.

6.9.10. Otras formas de divulgación de información de revocación disponibles

Algunas PC pueden dar soporte a otras formas de aviso de revocación, como los Puntos de Distribución de CRLs (CDP).

6.9.11. Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

6.9.12. Causas para la suspensión

La suspensión de la vigencia de los certificados únicamente se aplicará a los certificados personales, entre otros en los siguientes casos:

- Cambio temporal de alguna de las características del titular del certificado que aconsejen la suspensión de los certificados durante el periodo de cambio. Al retornarse a la situación inicial

se levantará la suspensión del certificado. Las características y requisitos para la suspensión se establecerán en la correspondiente Política de Certificación.

- Comunicación por el titular del certificado de un posible compromiso de sus claves. En el caso de que la sospecha, por su grado de certeza, no aconseje la revocación inmediata, se suspenderán los certificados del titular mientras se averigua el posible compromiso de las claves. Al término del análisis se determinará si se revocan los certificados o si se levanta la suspensión

6.9.13. Quién puede solicitar la suspensión

La solicitud puede iniciarla el titular del certificado o el Administrador que se establezca en la PC correspondiente.

6.9.14. Procedimiento para la solicitud de suspensión

La solicitud de suspensión la tramitará el Administrador mediante la transacción que se establezca al efecto en el sistema de Administración. Por el mismo método se solicitará el levantamiento de la suspensión cuando éste proceda.

En cualquier caso, se le comunicará al titular del certificado tanto la suspensión del mismo como su cese por correo electrónico.

6.9.15. Límites del periodo de suspensión

Por defecto INDRAPKI suspenderá la vigencia de los certificados por un plazo máximo de sesenta (60) días hábiles, plazo tras el cual se revocará el Certificado, salvo que se hubiera levantado previamente la suspensión del certificado.

Si durante el tiempo de suspensión del Certificado éste caduca o se solicita su revocación, se producirán las mismas consecuencias que para los Certificados no suspendidos, en esos mismos casos de caducidad o revocación.

6.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

6.10.1. Características operativas

INDRAPKI dispone de modo general de dos servicios que proporcionan información sobre el estado de los certificados emitidos por su AC:

- Publicación de las Listas de Certificados Revocados (CRL). El acceso a las CRL se puede hacer vía Active Directory (sólo Terceros Aceptantes ubicados en la red interna de INDRA) y HTTP (todas los Terceros Aceptantes).

6.10.2. Disponibilidad del servicio

El servicio, en sus dos variantes, está disponible de forma ininterrumpida todos los días del año, tanto para los Terceros Aceptantes internos de INDRA como para los Terceros Aceptantes externos.

6.10.3. Características adicionales

No estipulado.

6.11. EXTINCIÓN DE LA VALIDEZ DE UN CERTIFICADO

La extinción de la validez de un certificado se puede dar de dos formas:

- Revocación anticipada del certificado por cualquiera de las causas recogidas en el apartado 6.9.1.
- Expiración de la vigencia del certificado.

Si no se solicita la renovación del certificado la extinción de su validez supondrá la extinción de la relación entre el titular y la AC.

6.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

6.12.1. Prácticas y políticas de custodia y recuperación de claves

En cada PC donde se establezca el archivo de claves privadas se identificarán las políticas y prácticas para el registro y recuperación de claves.

Como norma general, no se archivará la clave privada de ningún certificado que tenga autorizada la funcionalidad de firma electrónica no repudiable. Esto se podrá comprobar verificando que la extensión 'Key Usage' tenga el código igual a 1 en el campo 'Non Repudiation'.

6.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

En los casos en que sea de aplicación, la PC correspondiente identificará las políticas y prácticas para la protección y recuperación de la clave de sesión.

7. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

7.1. CONTROLES FÍSICOS

7.1.1. Ubicación física y construcción

Los edificios donde se encuentra ubicada la infraestructura de INDRAPKI disponen de medidas de seguridad de control de acceso, de forma únicamente se garantiza la entrada a los mismos a las personas debidamente autorizadas.

Todas las operaciones críticas de INDRAPKI se realizan en recintos físicamente seguros, con niveles de seguridad específicos para los elementos más críticos.

Los Centros de Proceso de Datos de INDRAPKI cumplen los siguientes requisitos físicos:

a) Están alejados de salidas de humos para evitar posibles daños por incendios en otras plantas.

b) Ausencia de ventanas al exterior del edificio.

c) Detectores de intrusión y cámaras de vigilancia en las áreas de acceso restringido.

d) Control de acceso basado en tarjeta y contraseña.

e) Sistemas de protección y prevención de incendios: detectores, extintores, formación del personal para actuar ante incendios, etc.

f) Existencia de mamparas transparentes, limitando las distintas zonas, que permitan observar las salas desde pasillos de acceso, para detectar intrusiones o actividades ilícitas en su interior.

g) Protección del cableado contra daños e interceptación tanto de la transmisión de datos como de telefonía.

7.1.2. Acceso físico

Se dispone de un completo sistema de control de acceso físico de personas a la entrada. Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro.

Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios humanos y técnicos.

7.1.3. Alimentación eléctrica y aire acondicionado

Las salas donde se ubican los equipos de la infraestructura de INDRAPKI disponen de suministro de electricidad y aire acondicionado adecuado a los requisitos de los equipos en ellas instalados. La infraestructura está protegida contra caídas de tensión o cualquier anomalía en el suministro eléctrico. Aquellos sistemas que lo requieren disponen de unidades de alimentación permanente así como de grupo electrógeno.

7.1.4. Exposición al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado.

7.1.5. Protección y prevención de incendios

Las salas disponen de los medios adecuados - detectores- para la protección de su contenido contra incendios.

El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados - detectores en suelo y techo- para la protección del mismo contra incendios.

7.1.6. Sistema de almacenamiento

INDRAPKI ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

INDRAPKI ha dispuesto planes de copia de respaldo, los mismos que para el resto de la infraestructura central de INDRA, de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.

7.1.7. Eliminación de residuos

Se ha adoptado una política de gestión de residuos que garantiza la destrucción de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

7.1.8. Copias de seguridad fuera de las instalaciones

INDRAPKI dispone de copias de seguridad en dos locales propios que reúnen las medidas precisas de seguridad y con una separación física adecuada.

7.2. CONTROLES DE PROCEDIMIENTO

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se incluye una parte de la misma.

INDRAPKI procura que toda la gestión, tanto los procedimientos operacionales como de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorias periódicas.

Asimismo, se ha diseñado una segregación de funciones para evitar que una sola persona pueda conseguir el control total de la infraestructura.

7.2.1. Roles responsables del control y gestión de la PKI

Se distinguen los siguientes responsables para el control y gestión del sistema:

- **Administrador de PKCS#12 del archivo de claves**: Es el único que tiene las facultades para recuperar del archivo de claves las claves de cifrado de un usuario.
- **Administrador de contraseñas del archivo de claves**: Es el único que tiene las facultades para recuperar del archivo de claves la contraseña del PKCS#12 de cifrado de un usuario.
- **Operador de ARP (Autoridad de Registro Presencial)**: Las tareas de Administración / Gestión del ciclo de vida de los certificados emitidos por la AC serán llevadas a cabo por parte de los operadores de ARP. Estos operadores se encargarán de la:
  - Emisión de certificados para usuarios
  - Emisión de certificados para servidores
  - Emisión de certificados para componentes
  - Control de la aceptación de las condiciones de uso por parte de los usuarios
  - Revocación y suspensión de certificados
  - Suspensión de Servicios
- **Administrador de Sistemas**: responsable del funcionamiento de los sistemas que componen la PKI, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de Base de Datos, del repositorio de información y de los sistemas operativos.
- **Coordinador de Seguridad**: responsable de la definición y verificación de todos los procedimientos de seguridad tanto física como informática.
- **Autoridad de Aprobación de Políticas (AAP)**: autoridad responsable de la definición y aprobación de las políticas de certificación.
- **Administrador de Auditoria**: responsable de las tareas de ejecución y revisión de auditorías internas del sistema.
- **Administrador de Backup**: responsable de las tareas de ejecución y revisión de las copias de seguridad del sistema.

7.2.2. Número de personas requeridas por tarea

Se requiere una persona con capacidad profesional suficiente para realizar las tareas recogidas en cada uno de los roles planteados en el apartado anterior.

7.2.3. Identificación y autenticación para cada usuario

Los usuarios autorizados de INDRAPKI se identifican mediante certificados electrónicos emitidos por la propia PKI.

7.2.4. Roles que requieren segregación de funciones

La asignación de personal garantizará que más de una función especificada en el apartado 5.2.1 NO recaiga sobre la misma persona. Los roles que poseen segregación de funciones son:

- Recuperación de claves del archivo de claves
- Administrador de Auditoría

7.3. CONTROLES DE PERSONAL

7.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Todo el personal que preste sus servicios en el ámbito de la INDRAPKI deberá poseer el conocimiento, la experiencia y formación suficientes, para el mejor cometido de las funciones asignadas.

Para ello, INDRA podrá llevar a cabo los procesos de selección de personal que estime precisos con objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

7.3.2. Procedimientos de comprobación de antecedentes

Según los procedimientos de selección de personal establecidos por INDRA.

7.3.3. Requerimientos de formación

Según los procedimientos establecidos por INDRA.

En particular, el personal relacionado con la explotación de la PKI, recibirá la formación necesaria para asegurar la correcta realización de sus funciones. Se incluyen en la formación los siguientes aspectos:

- Entrega de una copia de la Declaración de Prácticas de Certificación.
- Concienciación sobre la seguridad física, lógica y técnica.
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos para la recuperación de la operación de la PKI en caso de desastres.

7.3.4. Requerimientos y frecuencia de actualización de la formación

Según los procedimientos establecidos por INDRA.

7.3.5. Frecuencia y secuencia de rotación de tareas

No estipulado.

7.3.6. Sanciones por acciones no autorizadas

La comisión de acciones no autorizadas será valorada como falta laboral y sancionada conforme a lo preceptuado en el Reglamento de Trabajo de INDRA y en el Estatuto de los Trabajadores, sin perjuicio de las responsabilidades de otra índole en que pudiera incurrirse.

7.3.7. Requisitos de contratación de terceros

Se aplicará la normativa general de INDRA para las contrataciones.

7.3.8. Documentación proporcionada al personal

Se facilitará el acceso a la normativa de seguridad de obligado cumplimiento junto con la presente DPC y las contenidas en las PC que sean de aplicación.

7.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

7.4.1. Tipos de eventos registrados

Las operaciones se dividen en eventos, por lo que se guarda información sobre uno o más eventos para cada operación relevante. Los eventos registrados poseen la información siguiente:

Categoría: Indica la importancia del evento.

- *Informativo*: los eventos de esta categoría contienen información sobre operaciones realizadas con éxito.
- *Marca*: cada vez que empieza y termina una sesión de administración, se registra un evento de esta categoría.
- *Advertencia*: indica que se ha detectado un hecho inusual durante una operación, pero que no provocó que la operación fallara (p.ej. una petición de lote denegada).
- *Error*: indica el fallo de una operación debido a un error predecible (p.ej. un lote que no se ha procesado porque la AR pidió una plantilla de certificación para la cual no estaba autorizada).
- *Error Fatal*: indica que ha ocurrido una circunstancia excepcional durante una operación (p.e. una tabla de base de datos a la que no se puede acceder).

Fecha: Fecha y hora en la que ocurrió el evento.

Autor: Nombre distintivo de la Autoridad que generó el evento.

Rol: Tipo de Autoridad que generó el evento.

Tipo evento: Identifica el tipo del evento, distinguiendo, entre otros, los eventos criptográficos, de interfaz de usuario, de librería.

Id. Evento: Número que identifica exclusivamente a un evento de entre un grupo de eventos del mismo tipo, generados por un mismo módulo.

Módulo: Identifica el módulo que generó el evento. Los posibles módulos son:

- AC.
- AR.
- Repositorio de información.
- Librerías de control de almacenamiento de información.

Nivel: Número que indica el nivel en que se encuentra el evento. Los eventos producidos por algunas operaciones están organizados de forma jerárquica, por lo que un evento puede agrupar otros eventos de nivel inferior, en función de la complejidad de la operación. Para eventos de primer nivel, este campo indicará un valor de 1. Para los de segundo nivel, y sucesivos, indicará el valor correspondiente. Se asignará un valor de 0 a los eventos en los que esta característica no sea aplicable.

Observaciones: Representación textual del evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyos valores variarán dependiendo de los datos sobre los que se ejecutó la operación.

Algunos ejemplos de los parámetros que se incluyen para la descripción del evento "Certificado generado" son: el número de serie, el nombre distintivo del titular del certificado emitido y la plantilla de certificación que se ha aplicado.

Los eventos registrados en la Base de Datos pueden estar sujetos al tipo de certificado, quedando especificado en la correspondiente Política de Certificación.

7.4.2. Frecuencia de procesado de registros de auditoría

Los registros se analizarán de manera manual cuando sea necesario, no existiendo una frecuencia definida para dicho proceso.

7.4.3. Periodo de conservación de los registros de auditoría

La información generada por los registros de auditoria se mantiene en línea hasta que es archivada. Una vez archivados, los registros de auditoria se conservarán, al menos, durante 2 años.

7.4.4. Protección de los registros de auditoría

Los eventos registrados por la PKI están protegidos mediante cifrado, de forma que nadie, salvo las propias aplicaciones de visualización de eventos (con su debido control de accesos), pueda acceder a ellos.

La destrucción de un archivo de auditoria solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorias de INDRAPKI. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres Autoridades o del administrador del servicio auditado.

7.4.5. Procedimientos de respaldo de los registros de auditoría

Las copias de respaldo de los registros de auditoria se realizan según las medidas estándar establecidas por INDRA para las copias de respaldo de las Bases de Datos de los Ordenadores Centrales.

7.4.6. Sistema de recogida de información de auditoría (interno vs externo)

El sistema de recopilación de información de auditoria de la PKI es una combinación de procesos automáticos y manuales ejecutados por las aplicaciones de la PKI. Todos los registros de auditoria de las ACs, LRAs se almacenan en los sistemas internos de INDRAPKI.

Todos los elementos significativos existentes en INDRAPKI se acumulan en una Base de Datos. Los procedimientos de control de seguridad empleados en INDRAPKI se basan en la tecnología de construcción empleada en la base de datos.

Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.
- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.
- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él. Esto permite guardar un registro de las operaciones realizadas y evita que se pierdan firmas electrónicas realizadas anteriormente por otros usuarios cuando se actualizan los datos.

La siguiente tabla es un resumen de los posibles peligros a los que una base de datos puede estar expuesta y que pueden detectarse con las pruebas de integridad.

- Inserción o alteración fraudulenta de un registro de sesión.
- Supresión fraudulenta de sesiones intermedias.
- Inserción, alteración o supresión fraudulenta de un registro histórico de una sesión cerrada.
- Inserción, alteración o supresión fraudulenta de un registro histórico de una sesión abierta y activa.
- Se dice lo mismo que en el punto anterior.
- Supresión fraudulenta de los registros históricos intermedios de una sesión no-cerrada e inactiva.
- Inserción, alteración o supresión fraudulenta del registro de una tabla de consultas.

7.4.7. Notificación al sujeto causa del evento

No se prevé la notificación automática de la acción de los ficheros de registro de auditoria al causante del evento.

7.4.8. 5.4.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto con el Plan de Auditoria de INDRA

7.5. ARCHIVO DE REGISTROS

7.5.1. Tipo de eventos archivados

Cada Autoridad de Certificación definida en INDRAPKI conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, manteniendo un registro de eventos. Esta información se conserva en particular con el objeto de poder proporcionar pruebas ciertas de la certificación en el marco de actuación de procedimientos legales.

Las operaciones registradas incluyen las realizadas por los administradores que utilizan las aplicaciones de administración de los elementos de INDRAPKI, así como toda la información relacionada con el proceso de registro.

Los tipos de datos o ficheros que son archivados son, entre otros, los siguientes:

- Datos relacionados con el procedimiento de registro y solicitud de certificados.
- Los especificados en el punto 7.4.4.
- El fichero histórico de claves.

7.5.2. Periodo de conservación de registros

Toda la información y documentación relativa a los certificados se conservarán durante 15 años, plazo que en el caso de los certificados reconocidos deriva de un mandato legal.

Para los registros de auditoria se estará a lo especificado en el apartado 7.4.3, siempre atendiendo a cualquier particularidad especificada en la Política de Certificación del Certificado correspondiente a los datos involucrados.

7.5.3. Protección del archivo

El especificado en el apartado 7.4.4, siempre atendiendo a cualquier particularidad especificada en la Política de Certificación del Certificado correspondiente a los datos involucrados.

7.5.4. Procedimientos de copia de respaldo del archivo

Igual a lo especificado en el apartado 7.4.5 para los archivos de registros de auditoría.

7.5.5. Requerimientos para el sellado de tiempo de los registros

Los sistemas de información empleados por INDRAPKI garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. Todos los sistemas sincronizan su instante de tiempo con esta fuente.

7.5.6. Sistema de archivo de información de auditoría (interno vs externo)

El sistema de recogida de información es interno a la Autoridad y corresponde a la INDRAPKI.

7.5.7. Procedimientos para obtener y verificar información archivada

Los eventos registrados por la PKI están protegidos mediante cifrado, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos.

Esta verificación debe ser llevada a cabo por el Administrador de Auditoria que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la PKI.

7.6. CAMBIO DE CLAVES

Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de AC a los titulares y Terceros Aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el repositorio de INDRAPKI.

7.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O CATÁSTROFE

7.7.1. Procedimientos de gestión de incidentes y compromisos

INDRA tiene establecido un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por INDRAPKI.

Este plan se engloba dentro del Plan de Contingencias de Sistemas Internos.

En el caso de que se produjera un compromiso de los datos de verificación de firma de alguna Autoridad de Certificación, INDRAPKI informará a todos los titulares de certificados de INDRAPKI y Terceros Aceptantes conocidos que todos los Certificados y Listas de Revocación firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio y en las nuevas condiciones aplicables.

7.7.2. Alteración de los recursos hardware, software y/o datos

Si los recursos hardware, software, y/o datos se alteran o se sospecha haber sido alterados se detendrá el funcionamiento de la PKI hasta que se reestablezca la seguridad del entorno con la incorporación de nuevos componentes de eficiencia que puedan acreditarse. De forma simultánea se realizará una auditoria para identificar la causa de la alteración y asegurar su no reproducción.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

7.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

En el caso de compromiso de la clave de una Autoridad se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente CRL, cesando el funcionamiento de actividad de la Autoridad y se procederá a la generación, certificación y puesta en marcha de una nueva Autoridad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso que la Autoridad afectada sea una AC el certificado revocado de la Autoridad permanecerá accesible en el repositorio de INDRAPKI con objeto de continuar verificando los certificados emitidos durante su periodo de funcionamiento.

Las Autoridades componentes de INDRAPKI dependientes de la nueva Autoridad serán informadas del hecho y conminadas a solicitar una nueva certificación por la nueva Autoridad.

Los certificados firmados por Autoridades dependientes de la comprometida en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informados sus usuarios de tal hecho y se procederá a la emisión de nuevos certificados.

Se comunicará a todas las Autoridades afectadas que los certificados y la información sobre su revocación, suministrada con la clave comprometida de la AC, deja de ser válida desde el momento de su notificación, debiendo utilizar la suministrada sirviéndose para ello de la nueva clave.

7.7.4. Instalación después de un desastre natural u otro tipo de catástrofe

El sistema de Autoridades de Certificación de INDRAPKI puede ser reconstruido en caso de desastre. Para llevar a cabo esta reconstrucción es necesario contar con:

- Una copia de respaldo de los discos del sistema anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la AC, incluidas sus claves privadas.

El almacenado se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de desastres en los sistemas en producción y en los elementos de recuperación.

7.8. CESE DE UNA AC O AR

7.8.1. Autoridad de Certificación

En el caso de cesar la actividad una de las AC de INDRAPKI se asegurará que los potenciales problemas para los titulares de sus certificados y los Terceros Aceptantes sean los mínimos, así como el mantenimiento de los registros requeridos para proporcionar prueba cierta de la certificación a efectos legales.

En caso de cese de la actividad de una o de todas sus ACs de INDRAPKI, esta comunicará a los titulares de sus certificados, por cualquier medio que garantice el envío y la recepción de la notificación y con un plazo mínimo de antelación de 2 meses a su fecha de su extinción, su intención de que la/s AC correspondientes cesan en la actividad como prestadores de servicios de certificación.

En el supuesto de que INDRAPKI decidiera transferir la actividad a otro Prestador de Servicios de Certificación, comunicará al titular de sus certificados los acuerdos de transferencia. A tal efecto INDRAPKI enviará un documento explicativo de las condiciones de transferencia y de las características del Prestador al que se propone la transferencia de la gestión de los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de 2 meses al cese efectivo de su actividad.

INDRAPKI podrá transferir, con el consentimiento expreso de sus titulares, la gestión de los certificados que sigan siendo válidos en la fecha en que el cese se produzca.

Transcurrido el plazo de dos meses, sin que exista acuerdo de transferencia o sin que el suscriptor acepte expresamente la misma, los certificados serán revocados.

7.8.2. Autoridad de Registro

Una vez la Autoridad de Registro cese en el ejercicio de las funciones, transferirá los registros que mantenga a INDRAPKI, mientras exista la obligación de mantener archivada la información, y de no ser así, esta será destruida.

8. CONTROLES DE SEGURIDAD TÉCNICA

8.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

8.1.1. Generación del par de claves

Los pares de claves para los componentes internos de INDRAPKI, concretamente *INDRA AC RAIZ V2, INDRA AC CORPORATIVA V2, INDRA Archivo de Claves e INDRA Recuperación de Claves,* se generan internamente en la base de datos de las respectivas ACs. Los sistemas de hardware y software que se emplean son conformes a las normas ESSI CWA 14167-1 y CWA 14167-2.

Los pares de claves para el resto de titulares se generan en función de lo estipulado en la Política de Certificación aplicable a cada certificado.

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por INDRAPKI vienen definidos por la Política de Certificación que le sea de aplicación.

8.1.2. Entrega de la clave privada al titular

El método de entrega de la clave privada a sus titulares depende de cada certificado y será establecido en la Política de Certificación correspondiente a cada certificado.

8.1.3. Entrega de la clave publica al emisor del certificado

El método de entrega de la clave pública al emisor en los casos en que la genere el Titular dependerá de cada certificado y será establecido en la Política de Certificación correspondiente.

8.1.4. Entrega de la clave pública de la AC a los terceros aceptantes

La clave pública de las AC se está a disposición de los Terceros Aceptantes en el Repositorio de INDRAPKI sin perjuicio de que una PC pueda establecer mecanismos adicionales de entrega de dichas claves.

8.1.5. Tamaño de las claves

El tamaño de las claves de *INDRA AC RAIZ V2* y de *INDRA AC CORPORATIVA V2* es de 2048 bits.

El tamaño de las claves para cada tipo de certificado emitido por INDRAPKI viene definido por la Política de Certificación que le sea de aplicación.

8.1.6. Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de *INDRA AC Raíz* y de *INDRA AC Corporativa* está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el *RSA*.

Los parámetros de generación de claves para cada tipo de certificado emitido por INDRAPKI vienen definidos en la Política de Certificación que le sea de aplicación.

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por INDRAPKI vienen definidos por la Política de Certificación que le sea de aplicación.

8.1.7. Fines del uso de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para cada tipo de certificado emitido por INDRAPKI vienen definido por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por INDRAPKI contienen la extensión *Key Usage* definida por el estándar X.509 v3, la cual se califica como crítica. Asimismo, pueden establecerse limitaciones adicionales mediante la extensión *Extended Key Usage*.

Se ha de tener en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por INDRAPKI

8.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

8.2.1. Estándares para los módulos criptográficos

No estipulado.

8.2.2. Control multipersona (k de n) de la clave privada

No estipulado.

8.2.3. Custodia de la clave privada

No estipulado.

8.2.4. Copia de seguridad de la clave privada

No estipulado.

8.2.5. Archivo de la clave privada

Las claves privadas de firma de personas nunca serán archivadas. Sólo se archivarán las claves de cifrado, debiéndose establecer en su PC el procedimiento de recuperación.

8.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

No estipulado.

8.2.7. Almacenamiento de la clave privada en un módulo criptográfico

No estipulado.

8.2.8. Método de activación de la clave privada

No estipulado.

8.2.9. Método de desactivación de la clave privada

No estipulado.

8.2.10. Método de destrucción de la clave privada

No estipulado.

8.2.11. Clasificación de los módulos criptográficos

No estipulado

8.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

8.3.1. Archivo de la clave pública

INDRAPKI mantiene un archivo de todos los certificados, los cuales incluyen las claves públicas, emitidos por un periodo de quince (15) años. El control de dicho registro está a cargo de los Administradores de cada una de las ACs de INDRAPKI.

El archivo dispone de medios de protección frente a las manipulaciones que pretendan efectuarse sobre la información contenida.

8.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves

El certificado y el par de claves *de INDRA AC RAÍZ V2* de INDRAPKI tienen una validez de treinta (30) años y los de *INDRA AC CORPORATIVA V2* de INDRAPKI de quince (15) años.

El periodo de validez del resto de certificados vendrá establecido por la Política de Certificación aplicable a cada uno..

8.4. DATOS DE ACTIVACIÓN

8.4.1. Generación e instalación de los datos de activación

No estipulado.

8.4.2. Protección de los datos de activación

No estipulado.

8.4.3. Otros aspectos de los datos de activación

No estipulado.

8.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Los datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

8.5.1. Requerimientos técnicos de seguridad específicos

Los datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

8.5.2. Evaluación de la seguridad informática

INDRAPKI evalúa de forma permanente su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorias externas e internas, así con la realización continua de controles de seguridad.

8.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Los datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

8.6.1. Controles de desarrollo de sistemas

Los requisitos de seguridad se consideran, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de INDRAPKI

8.6.2. Controles de gestión de seguridad

Existe una organización de seguridad encargada de su gestión.

8.6.3. Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas con algún impacto en la seguridad de INDRAPKI.

8.7. CONTROLES DE SEGURIDAD DE LA RED

Los datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

8.8. SELLADO DE TIEMPO

No estipulado.

9. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

9.1. PERFIL DE CERTIFICADO

9.1.1. Número de versión

INDRAPKI soporta y utiliza certificados X.509 versión 3 (X.509 v3).

9.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *SubjectAlternativeName*. Calificada como no crítica.
- *CRLDistributionPoint*. Calificada como no crítica.

Las Políticas de Certificación de INDRAPKI pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

INDRAPKI tiene definida una política de asignación de OID's dentro de su arco privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de INDRAPKI comienzan con el prefijo 1.3.6.1.4.1.8173.2.3.

9.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

SHA-256 with RSA Encryption.

9.1.4. Formatos de nombres

Los certificados emitidos por INDRAPKI contienen el *distinguished name* X.500 del emisor y del titular del certificado en los campos *issuer name* y *subject name* respectivamente.

9.1.5. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a *distinguished names* X.500, únicos y no ambiguos.

9.1.6. Identificador de objeto (OID) de la Política de Certificación

A definir en cada Política de Certificación.

INDRAPKI tiene definida una política de asignación de OID's dentro de su arco privado de numeración por la cual el OID de todas las Políticas de Certificación de INDRAPKI comienzan con el prefijo **1.3.6.1.4.1. 8173**.2.2.

9.1.7. Uso de la extensión "PolicyConstraints"

No estipulado.

9.1.8. Sintaxis y semántica de los "PolicyQualifier"

No estipulado.

9.1.9. Tratamiento semántico para la extensión crítica "Certificate Policy"

La extensión será marcada como "nonCritical" cuando se emplee con el objeto de mantener la máxima capacidad de poder operar con otras AC del certificado. Esto se hace siguiendo las recomendaciones para aplicaciones estándar de correo electrónico seguro S/MIME [RFC 2632] y autenticación web SSL/TLS [RFC 2246]. El hecho de que la extensión no sea crítica no impide que las aplicaciones utilicen la información contenida en la citada extensión.

9.2. PERFIL DE CRL

9.2.1. Número de versión

INDRAPKI soporta y utiliza CRLs X.509 versión 2 (v2).

9.2.2. CRL y extensiones

No estipulado.

10. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

10.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Se llevará a cabo una auditoria sobre INDRAPKI de forma regular, de acuerdo con el Plan de Auditorias de INDRA. Con ello se garantiza la adecuación de su funcionamiento y operativa con las disposiciones incluidas en esta DPC y las PC.

Como mínimo se realizarán auditorías cada dos años, de acuerdo con lo que establece el Reglamento de Medidas de Seguridad (RD 994/1999) para los ficheros de nivel medio.

10.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

La realización de las auditorias podrá ser encargada a Empresas Auditoras Externas o al Departamento de Auditoría Interna en función de la disponibilidad de personal cualificado en los aspectos concretos a auditar y de lo que establezca el Plan de Auditorías.

Cualquier equipo o persona designada para realizar una auditoría de seguridad sobre INDRAPKI deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la autoridad de INDRAPKI.

10.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Al margen de la función de auditoría, el auditor externo y la parte auditada (INDRAPKI) no deberán tener relación alguna que pueda derivar en un conflicto de intereses. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoria.

10.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoria determinará la conformidad de los servicios de INDRAPKI con esta DPC y las PC's aplicables. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

El ámbito de actividad de una auditoria incluirá, pero no estará limitada a:

- Política de seguridad y privacidad

- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la AC
- Selección de personal
- DPC y PC's competentes
- Contratos

10.5. ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

La identificación de deficiencias detectadas como resultado de la auditoria dará lugar a la adopción de medidas correctivas. La Autoridad de Aprobación de Políticas (AAP), en colaboración con el auditor, será la responsable de la determinación de las mismas.

En el caso de observarse deficiencias graves la Autoridad Aprobadora de Políticas podrá adoptar, entre otras, las siguientes decisiones: suspensión temporal de las operaciones hasta que las deficiencia se corrija, revocación del certificado de la Autoridad, cambios en el personal implicado, invocación de la política de responsabilidades y auditorias globales más frecuentes.

10.6. COMUNICACIÓN DE RESULTADOS

El equipo auditor comunicará los resultados de la auditoria a la Autoridad Aprobadora de Políticas de INDRAPKI (AAP), al Gestor de Seguridad de INDRAPKI, así como a los administradores de INDRAPKI y de la Autoridad en la que se detecten incidencias.

11. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

11.1. TARIFAS

11.1.1. Tarifas de emisión de certificado o renovación

Las tarifas de emisión y renovación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

11.1.2. Tarifas de acceso a los certificados

Las tarifas de acceso a los certificados se especifican en la Política de Certificación que les sea de aplicación.

11.1.3. Tarifas de acceso a la información de estado o revocación

Las tarifas de acceso a la información de estado o revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

11.1.4. Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta DPC, ni las políticas de certificación administradas por INDRAPKI, ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

Esta disposición podrá ser modificada por la Política de Certificación aplicable en cada caso.

11.1.5. Política de reembolso

En el caso que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de INDRAPKI para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente.

11.2. RESPONSABILIDADES FINANCIERAS

11.2.1. Cobertura asegurada

Salvo que la PC establezca lo contrario los certificados emitidos por INDRAPKI no podrán ser utilizados para actividades con trascendencia económica por lo que no se establece una cobertura de seguros específica para su actividad.

11.2.2. Otros activos

INDRAPKI forma parte de INDRA disponiendo éste de solvencia financiera suficiente.

11.2.3. Cobertura de seguro u otras garantías para los terceros aceptantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI. Los certificados emitidos por las ACs de INDRAPKI no permiten realizar transacciones monetarias a menos que quede explícitamente definido en su correspondiente Política de Certificación. No obstante lo anterior aquellos certificados emitidos por las ACs de INDRAPKI que estén autorizados para la realización de transacciones económicas y que de un uso irregular de los mismos pueda inferirse daños a los Terceros Aceptantes, el pago de las indemnizaciones estará regulada en la Política de Certificación que corresponda, siempre que aquellos hayan comprobado las firmas electrónicas realizadas con los mismos y verificado su validez.

11.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Con independencia de lo establecido en el artículo 6 del Real Decreto-Legislativo 1298/1986, de 26 de junio, sobre el deber de confidencialidad de los datos e informaciones de las que disponga INDRA en el ejercicio de sus funciones, se establece el siguiente régimen de confidencialidad de los datos relativos a la INDRAPKI:

11.3.1. Ámbito de la información confidencial

Toda información que no sea considerada por INDRAPKI como pública revestirá el carácter de confidencial. Se declara expresamente como información confidencial:

- Las claves privadas de las Autoridades que componen INDRAPKI.
- Las claves privadas de titulares que INDRAPKI mantenga en custodia.
- La información relativa a las operaciones que lleve a cabo INDRAPKI.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- La información de carácter personal proporcionada por los titulares de certificados a INDRAPKI durante el proceso de registro, de conformidad con lo dispuesto en la normativa sobre protección de datos de carácter personal y reglas de desarrollo.

11.3.2. Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente Declaración de Prácticas de Certificación.
- La incluida en las Políticas de certificación que le sean de aplicación.
- Los certificados emitidos.
- La lista de los certificados suspendidos o revocados.

11.3.3. Responsabilidad de la protección de la información confidencial

Los empleados de INDRA que participen en cualesquiera tareas propias o derivadas de la INDRAPKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable recogida fundamentalmente en el Reglamento Interno de INDRA, aprobado por Resolución del Consejo de Gobierno, de 28 de marzo de 2000 y en la normativa convencional interna.

Asimismo el personal contratado que participe en cualquier actividad u operación de INDRAPKI estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con INDRA.

11.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

11.4.1. Política de protección de datos de carácter personal

De acuerdo con la legislación española al respecto, se recoge dentro del capítulo 12, apartado 12.1 y siguientes.

11.4.2. Información tratada como privada

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal.

11.4.3. Información no calificada como privada

En cada PC se establecerá qué datos personales se incluirán en los certificados y en los repositorios de acceso público (certificados y CRL). La aceptación por el titular afectado de la emisión del certificado emitido a su nombre equivale al consentimiento dado para su publicación

11.4.4. Responsabilidad de la protección de los datos de carácter personal

Esta responsabilidad se regula en el capítulo 12.

11.4.5. Comunicación y consentimiento para usar datos de carácter personal

En cada PC se establecerán los mecanismos por los que se comunicará y obtendrá, en su caso, el consentimiento del titular afectado para el tratamiento de los datos de carácter personal.

11.4.6. Revelación en el marco de un proceso judicial

Los datos de carácter personal solo podrán ser comunicados a terceros, sin consentimiento del afectado, únicamente en los supuestos contemplados en la legislación reguladora de protección de datos de carácter personal, y entre ellos, cuando la comunicación tenga por destinatarios los jueces y tribunales en el ejercicio de las funciones que tiene atribuidas.

11.4.7. Otras circunstancias de publicación de información

Estas posibles circunstancias se regulan en el capítulo 12.

11.5. DERECHOS DE PROPIEDAD INTELECTUAL

En los términos establecidos en el Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, INDRA es titular en exclusiva de todos los derechos relativos a los Certificados Electrónicos emitidos por INDRAPKI para personas físicas o jurídicas y procesos informáticos; a las Listas de Certificados Revocados; al contenido de la presente Declaración de Prácticas de Certificación y a las Políticas de Certificación. Asimismo, INDRA es titular de los derechos relativos a cualquier otro documento electrónico o de otro tipo, protocolos, programas de ordenador y hardware, archivos, directorios, bases de datos y servicios de consultas que sean generados y utilizados en el ámbito de actuación de la misma INDRAPKI.

Los identificadores de objeto (OIDs) utilizados son propiedad de INDRA y han sido registrados en Internet Assigned Number Authority (IANA) bajo la rama *iso.org.dod.internet.private.enterprise* (1.3.6.1.4.1-IANA-Registered Private Enterprises), habiéndose asignado el número **1.3.6.1.4.1. 8173** (INDRA). Esto puede ser consultado y comprobado en:

http://www.iana.org/assignments/enterprise-numbers

Queda prohibido, salvo acuerdo expreso con INDRA, el uso total o parcial de cualquiera de los OID asignados a INDRA salvo para los usos específicos con que se incluyeron en el Certificado o en el Directorio.

Los derechos de propiedad intelectual de INDRA enunciados más arriba le corresponden en cualquier ámbito territorial, a todos los efectos y por tiempo indefinido.

11.6. OBLIGACIONES Y RESPONSABILIDADES

11.6.1. Obligaciones y responsabilidades de la AC

Las AC que operan bajo la jerarquía de INDRAPKI deben asegurarse de que todas las obligaciones establecidas en este apartado se implementan según sea aplicable en las políticas de certificación. Cada AC es responsable del cumplimiento de sus obligaciones, según se prescriben en esta DPC, incluso aunque parte de su actividad sea realizada por subcontratistas. Asimismo, cada AC proporcionará sus servicios de forma consistente con esta DPC.

Las ACs que operan bajo la jerarquía de INDRAPKI tienen las siguientes obligaciones:

OAC.1	Realizar sus operaciones en conformidad con esta DPC.
OAC.2	Proteger sus claves privadas.
OAC.3	Emitir certificados en conformidad con las Políticas de Certificación que les sean de aplicación.
OAC.4	Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 v3 y con los requerimientos de la solicitud.
OAC.5	Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
OAC.6	No publicar los certificados de usuario.
OAC.7	Revocar los certificados en los términos de la sección “6.9 Revocación y suspensión de certificados” y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web referidos en el apartado ”4.1 Repositorios”, con la frecuencia estipulada en el punto “6.9.7 Frecuencia de emisión de CRLs”.
OAC.8	Publicar esta DPC y las PC aplicables en el sitio web referido en el apartado ”4.1 Repositorios”.
OAC.9	Efectuar las revisiones de esta DPC y de las PC de acuerdo con lo establecido en el apartado "11.12 Procedimientos de Cambios en las Especificaciones”.
OAC.10	Comunicar los cambios de esta DPC y de las PC de acuerdo con lo establecido en el apartado “9.12.2 Periodo y mecanismo de notificación”.
OAC.11	Conservar los acuerdos firmados (en papel o electrónicamente) con los solicitantes de certificados en los que estos se dan por enterados de sus obligaciones y derechos, consienten en el tratamiento de sus datos personales por la AC y confirman que la información proporcionada es correcta.
OAC.12	Garantizar la disponibilidad de las CRLs de acuerdo con las disposiciones de la sección “4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados” de la presente DPC.
OAC.13	En el caso que la AC proceda a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con las Políticas de certificación que les sean de aplicación.
OAC.14	Colaborar con las auditorias dirigidas por INDRAPKI para validar la renovación de las propias claves.
OAC.15	Operar de acuerdo con la legislación aplicable. En concreto con: ○ La Ley 59/2003, de 19 de diciembre, de Firma Electrónica ○ La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. ○ La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal
OAC.16	Proteger, en caso de haberlas, las claves bajo su custodia.
OAC.17	No almacenar en ningún caso los datos de creación de firma (clave privada) de los titulares de

	certificados emitidos con el propósito de utilizarse para firma electrónica (key usage = non repudiation), sean reconocidos o no.
OAC.18	En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ellas emitidos.
OAC.19	Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años.

11.6.2. Obligaciones de la AR

Las ARs operativas en la PKI de INDRA deben cumplir con las siguientes cláusulas:

OAR.1	Identificar y autenticar correctamente al Titular y/o Solicitante y a la organización que represente, conforme a los procedimientos que se establecen en esta DPC y en las Políticas de Certificación específicas para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.
OAR.2	Formalizar la expedición de Certificados con el Titular en los términos y condiciones que establezcan las Políticas
OAR.3	Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del Certificado y en el proceso de suspensión/revocación del mismo.
OAR.4	Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC.

11.6.3. Obligaciones de los titulares de los certificados

Es obligación de los Titulares de los certificados emitidos bajo la presente política:

OTC.1	Suministrar a las Autoridades de Registro información que consideren exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.
OTC.2	Informar a los responsables de INDRAPKI de cualquier modificación de esta información.
OTC.3	Conocer y aceptar las condiciones de utilización de los certificados, en particular esta DPC y las PC que le sean de aplicación, así como las modificaciones que se realicen sobre las mismas. En particular, los certificados personales sólo podrán utilizarse mediante dispositivos seguros de creación de firma.
OTC.4	Limitar y adecuar el uso del certificado a propósitos lícitos y acordes con los usos permitidos por la Política de Certificación pertinente y la presente DPC.
OTC.5	Poner el cuidado y medios necesarios para garantizar la custodia de su clave privada, evitando su pérdida, divulgación, modificación o uso no autorizado.
OTC.6	Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada (ya sea por pérdida, robo, compromiso potencial, conocimiento por terceros del PIN, detección de inexactitudes en la información, etc.) correspondiente a la clave pública contenida en el certificado. Los modos en que puede realizarse esta solicitud se encuentran especificados en el apartado 4.9.3.
OTC.7	Destruir el Certificado cuando así lo exija la AC, en virtud del derecho de propiedad que en todo caso conserva sobre el Certificado, y cuando el Certificado caduque o sea revocado.
OTC.8	No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación, sin permiso previo por escrito de la Autoridad de Certificación.

OTC.9	Cualquier otra que se derive de la ley, de esta DPC o de las Políticas de Certificación.

11.6.4. Obligaciones de los terceros aceptantes

Es obligación de los terceros que acepten y confíen en los certificados emitidos por INDRAPKI:

OTA.1	Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
OTA.2	Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos (comprobando que el certificado en el que pretende confiar es válido y no ha caducado o ha sido suspendido o revocado).
OTA.3	Asumir su responsabilidad en la correcta verificación de las firmas electrónicas
OTA.4	Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
OTA.5	Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas
OTA.6	Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

11.6.5. Obligaciones de otros participantes

OOP.1	El Servicio de Repositorio ha de mantener accesible para las Entidades Finales la información de los certificados que han sido revocados, en formato CRL.

11.7. LIMITACIONES DE RESPONSABILIDADES

INDRAPKI no asumirá responsabilidad alguna en relación al uso de los Certificados emitidos por las ACs de INDRAPKI y el par de claves privada/pública asociado a sus titulares para cualquier escenario no especificado en esta DPC o en las Políticas de Certificación correspondientes.

INDRAPKI sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

INDRAPKI no se desempeña como agente fiduciario, fideicomisario, ni representante en forma alguna de usuarios ni de Terceros Aceptantes en los certificados que emite. INDRAPKI no realizará representaciones ante contrario, ni expresa ni implícitamente, ni en persona ni de otra manera.

11.8. DELIMITACIÓN DE RESPONSABILIDADES

Las ACs de INDRAPKI no asumen ninguna responsabilidad en caso de pérdida o perjuicio:

RESP.1	De los servicios que prestan, en caso de guerra, desastres naturales o cualquier otro caso de fuerza mayor (alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible).
RESP.2	Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario
RESP.3	Ocasionados durante el periodo comprendido entre la revocación de un certificado y la momento de publicación de la siguiente CRL
RESP.4	Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta DPC.
RESP.5	Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por INDRAPKI
RESP.6	Ocasionados por el uso de la información contenida en el certificado.
RESP.7	La AC no será responsable del contenido de aquellos documentos firmados electrónicamente ni de aquellas "páginas web" que contengan un certificado emitido por ella.

11.9. LIMITACIONES DE PÉRDIDAS

A excepción de lo establecido por las disposiciones de la presente DPC, INDRAPKI no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asumen ninguna otra responsabilidad ante usuarios o Terceros Aceptantes.

11.10. PERIODO DE VALIDEZ

11.10.1. Plazo

Esta DPC entra en vigor desde el momento de su aprobación por la AAP y su publicación en el repositorio de INDRAPKI.

Esta DPC está en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC RAIZ V2, ocasión en que obligatoriamente se emitirá una nueva versión.

11.10.2. Finalización

Esta DPC será siempre sustituida por una nueva versión con independencia de la magnitud de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la DPC quede derogada se retirará del repositorio público de INDRAPKI, si bien se conservará durante 15 años.

11.10.3. Efectos de la finalización y supervivencia

Las obligaciones y restricciones que establece esta DPC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de INDRAPKI, subsistirán tras el final de la vida de esta DPC.

11.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas descritas en esta DPC se realizará mediante mensaje electrónico o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto “1.5 Administración de las políticas”. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

11.12. PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES

11.12.1. Procedimiento para los cambios

Ocasionalmente INDRAPKI puede realizar modificaciones en sus Políticas de Certificación o en la presente DPC.

La Autoridad con atribuciones para realizar y aprobar cambios sobre la DPC y las PCs de INDRAPKI es la Autoridad de Aprobación de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado “3.5 Administración de las políticas” de esta DPC.

11.12.2. Periodo y mecanismo de notificación

En el caso que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se comunicará a los usuarios de los certificados correspondientes a la PC o DPC modificada que se ha efectuado un cambio y que deben consultar la nueva DPC en el repositorio establecido. El mecanismo de comunicación será el correo electrónico si afecta a esta DPC y el que establezca en su caso cada PC.

11.12.3. Circunstancias en las que el OID debe ser cambiado

Algunos de esos cambios no reducirán materialmente la confianza que una Política de Certificación o su implementación proporcionan, y se juzgarán por la AAP como que no modifican la aceptabilidad de los certificados que soporta la política para los propósitos para los que se han usado. En tales casos se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados correspondientes a la PC o DPC modificada.

En el caso que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del de Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los usuarios de los certificados correspondientes a la PC o DPC modificada.

11.13. PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS

Todas las querellas y reclamaciones entre usuarios y INDRAPKI en cualquiera de los entornos de certificación, antes de recurrir a cualquier mecanismo de resolución de disputas, incluyendo litigación y arbitrio, deberá ser comunicada por la parte en disputa a la Autoridad de Aprobación de Políticas (AAP) de INDRA y a las otras partes, si las hubiera, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir en relación a esta DPC o a las Políticas de Certificación, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los juzgados y tribunales de la ciudad de Madrid.

11.14. LEGISLACIÓN APLICABLE

Las operaciones y funcionamiento de INDRAPKI, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

De igual manera, habrán de observarse las normas y procedimientos internos dictados por INDRA encaminadas a garantizar el nivel de seguridad exigido por el Real Decreto citado en los casos en que sean de aplicación.

11.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

Es responsabilidad de la Autoridad de Aprobación de Políticas velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

11.16. ESTIPULACIONES DIVERSAS

11.16.1. Cláusula de aceptación completa

Todos los Terceros Aceptantes asumen en su totalidad el contenido de la última versión de esta DPC y de las PC que sean de aplicación en su uso y confianza en los certificados electrónicos sujetos a las mismas. Esta asunción de la última versión de la DPC y de las PC anula cualquier acuerdo previo oral o escrito en relación a la misma materia que sea contradictorio.

11.16.2. Independencia

El titular al que le haya sido asignado un certificado no puede transferirlo en ningún caso a un tercero, ni delegar sus responsabilidades sobre el mismo.

En el caso que una o más cláusulas de esta DPC sea o llegase a ser inválida, ilegal, o inexigible legalmente, tal inaplicabilidad no afectará a ninguna otra cláusula, sino que se actuará entonces como si las cláusula o cláusulas inaplicables nunca hubieran sido contenidas por esta DPC, y en tal grado como sea posible se interpretará la DPC para mantener la voluntad original de la misma.

Se entiende y acuerda de forma expresa por las partes afectadas por esta DPC, que todas y cada una de las disposiciones de regulan limitaciones de responsabilidad, renuncia de, limitaciones sobre cualquier garantía u otras limitaciones o exclusiones por daños y perjuicios, serán entendidas por separado.

11.16.3. Resolución por la vía judicial

No estipulado

11.17. OTRAS ESTIPULACIONES

No estipulado

12. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

12.1. RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS

Es de aplicación a la Política de Protección de Datos de Carácter Personal derivada de la presente Declaración de Prácticas de Certificación lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal y su normativa de desarrollo, entre la que cabe destacar el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal.

Sin menoscabo de otras obligaciones las Autoridades de Registro que se constituyan en INDRAPKI verificaran que el solicitante de un certificado es informado y presta su consentimiento al tratamiento de sus datos personales, a la finalidad que se les va a dar, a los destinatarios de los mismos y su inclusión en el fichero declarado al efecto por INDRAPKI.

En los casos en que los datos no hayan sido recabados directamente de los interesados, INDRAPKI o su representante informarán de forma expresa, precisa e inequívoca a estos, dentro de los tres meses siguientes al momento del registro de los datos, de lo recogido en el párrafo anterior.

El titular de los datos podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, dirigiéndose para ello a la dirección señalada en el siguiente apartado de la presente DPC.

Los datos contenidos en el Directorio seguro de Certificados tienen la consideración de datos de carácter personal a efectos de lo dispuesto en la LOPD y demás normativa complementaria, y por este motivo, INDRAPKI sólo permitirá el acceso de titulares de certificados a los mismos.

No obstante, INDRAPKI pone a disposición de las Entidades Finales las listas de certificados revocados (que no contiene datos personales) para el cumplimiento diligente de los servicios de certificación El usuario como cesionario de esta información únicamente podrá utilizarla de acuerdo con esas finalidades.

12.2. CREACIÓN DEL FICHERO E INSCRIPCIÓN REGISTRAL

Los datos de inscripción del fichero "PKI de INDRA" son:

- Nº de inscripción en el Registro General de Protección de Datos: PENDIENTE DE ASIGNACIÓN

Asimismo, el nombre del fichero, su área responsable y el área encargada de atender las peticiones de ejercicio de derechos son:

Nombre del Fichero	PENDIENTE DE ASIGNACIÓN
Responsable del Fichero	PENDIENTE DE ASIGNACIÓN
Atención de peticiones	PENDIENTE DE ASIGNACIÓN

12.3. DOCUMENTO DE SEGURIDAD LOPD

12.3.1. Aspectos cubiertos

Tal como se señala en el punto 1.1, la presente DPC se ha hecho de acuerdo a la especificación RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"* del Internet Engineering Task Force (IETF) para este tipo de documentos. Pero, la Ley 59/2003, de 19 de diciembre, de Firma Electrónica establece en su artículo 19.3 lo siguiente:

> *3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.*

Dado que lo que especifica el RFC 3647 mencionado no cubre todo lo demandado por el RD 994/1999 por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados con Datos de Carácter Personal, se hace necesario añadir el presente apartado para recoger en esta DPC todos los requisitos del mencionado Reglamento para los Documentos de Seguridad.

En consecuencia, en este capítulo se cubren los siguientes aspectos:

- Estructura básica de datos de carácter personal.
- Nivel de seguridad aplicable.
- Sistemas de Información que soportan el fichero
- Relación de usuarios
- Notificación y Gestión de Incidencias
- Copias de respaldo y recuperación
- Control de Accesos
- Ficheros Temporales
- Gestión de Soportes

El resto de aspectos que debe recoger un Documento de Seguridad han sido ya incluidos en capítulos anteriores de la presente DPC.

El objeto del Documento de Seguridad es preservar los datos de carácter personal procesados por INDRAPKI, por lo que afecta a todos aquellos recursos (personas, equipos, comunicaciones, software, procedimientos) implicados en el tratamiento de los datos.

Este documento es de obligado cumplimiento para todo el personal perteneciente a INDRAPKI, así como a todas aquellas personas relacionadas que requieran el acceso a datos de carácter personal.

12.3.2. Funciones y Obligaciones del personal

Esta DPC, así como futuras versiones de la misma son conocidas por todas las personas que accedan a los datos de carácter personal gestionados por INDRAPKI, siendo de obligado cumplimiento todas las funciones y obligaciones que establece.

12.3.3. Estructura de datos

Los datos incluidos en el fichero que trata INDRAPKI varían en función de si es un empleado de INDRA o una persona externa. En la siguiente tabla se recogen los datos tratados identificando cuando son de aplicación en cada caso:

DATOS TRATADOS	EMPLEADOS	TERCEROS
Datos de carácter identificativo		
D.N.I./N.I.F.		
NOMBRE Y APELLIDOS		
DIRECCIÓN (POSTAL, ELECTRÓNICA)		
Nº REGISTRO PERSONAL		
FIRMA ELECTRÓNICA		
Datos de características personales		
NACIONALIDAD		
Datos de detalles de empleo		
CATEGORIA / GRADO		
PUESTOS DE TRABAJO		

12.3.4. Nivel de Seguridad

Los datos tratados exigirían en nivel de seguridad básico, pero dadas las especiales características de seguridad que ha de tener una PKI y el nivel de seguridad que establece esta DPC (excede al marcado en el Reglamento para el nivel medio), se considera, a efectos de la declaración del fichero, que se le aplica el nivel medio de seguridad.

12.3.5. Sistemas de Información

Dentro de la estructura de sistemas de información que constituye INDRAPKI se pueden distinguir tres subsistemas con alguna implicación en el tratamiento de datos de carácter personal. A continuación se relacionan y describen de forma sintética:

- **Subsistema de Gestión de Certificados**

  Se encarga de la creación de los certificados conforme al estándar X.509v3, donde se introducen las claves generadas por el subsistema de generación de claves y otros datos identificativos que se definen en la correspondiente PC.

- **Subsistema de Autoridad de Registro**

  Se encarga de la identificación y autenticación del solicitante del certificado para proceder a la emisión posterior del certificado por INDRAPKI.

- **Subsistema de Publicación**

  Se encarga de la gestión de la publicación de las Listas de Revocados (CRL) y del Directorio de certificados.

12.3.6. Relación de usuarios

El Coordinador de Seguridad mantiene una relación de los usuarios con acceso a los datos tratados por la PKI en la que se indica su rol y nivel de acceso. Dicha relación de usuarios tiene carácter confidencial por motivos de seguridad, por lo que será precisa una petición motivada al Coordinador de Seguridad para tener acceso a la misma.

No se incluyen en esa relación los usuarios con acceso a los certificados electrónicos a efectos de hacer uso de los mismos para el envío de información cifrada ni los usuarios con acceso a las CRL.

12.3.7. Notificación y Gestión de Incidencias

Los procedimientos del Departamento de Sistemas Internos asociados a la gestión de problemas aseguran que todas las incidencias se registran y documentan, realizándose un seguimiento de las mismas. Se registra información relativa a: fecha, hora, tipo de incidencia, persona que comunica la incidencia, persona a quien se asigna la resolución de la incidencia, documentación sobre la causa y sus efectos.

Asimismo se han dado instrucciones al personal informático para que se documenten en el registro de incidencias los procedimientos utilizados para recuperar datos personales, indicando además qué persona realizó el proceso y qué datos han sido recuperados.

12.3.8. Copias de Respaldo y recuperación

Las copias de respaldo se realizan de forma diaria conforme a la normativa en vigor en INDRA al respecto para Ordenadores Centrales.

Las recuperaciones de datos se hacen con la autorización del responsable del fichero:

a. Incidencias en el sistema informático

   Se comunica al responsable informático del sistema, quien deberá obtener la autorización del propietario mediante los procedimientos establecidos al efecto.

b. Incidencias en la infraestructura del sistema informático (por ejemplo, discos)

   Se siguen los procedimientos establecidos en los planes de respaldo de la oficina de Informática, para cada contingencia.

12.3.9. Control de Accesos

Las autorizaciones de acceso a los sistemas de información estarán basadas exclusivamente en el principio de necesidad para el trabajo. Los administradores de usuarios y de elementos se encargarán de validar siempre esta necesidad antes de conceder el acceso a los datos.

Asimismo, todos los elementos que permitan acceder a datos personales estarán catalogados como de uso restringido.

12.3.10. Ficheros Temporales

El software utilizado para generar un certificado electrónico conforme al estándar X.509v3 genera ficheros temporales (ficheros de registros de auditoría) que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica 59/2003.

12.3.11. Gestión de Soportes

Los soportes internos están correctamente identificados por su código de barras o incluyen su correspondiente etiqueta identificativa.

Los soportes residen en las salas de ordenadores. El acceso a estas salas está restringido, las autorizaciones permanentes son validadas por el Jefe de Informática y el acceso provisional solo podrá ser autorizado por el Jefe de Explotación o el Jefe de Operación.

Toda salida de soportes fuera de los locales de INDRA deberá ser autorizada por el Administrador de la PKI. El Departamento de Sistemas Internos mantiene un registro en papel de la entrada/salida de soportes.

Los soportes que hubieran contenido datos personales se borrarán utilizando un borrado físico o procedimiento similar. Este proceso se realiza siempre que se reutilizan soportes que van a ser enviados al exterior; en otros casos no existe manipulación de soportes, ya que la gestión es realizada directamente por los robots que gestionan cartuchos.

Antes de autorizar la salida de soportes que contengan datos personales para operaciones de mantenimiento, se procede a su borrado físico o a su desmagnetización (salida de soportes por mantenimiento solo se daría en el caso de discos).

12.3.12. Utilización de datos reales en pruebas

No se utilizarán datos reales para la realización de pruebas, salvo que se aseguren los niveles de seguridad requeridos.

Los procedimientos de pruebas utilizados en el Departamento de Sistemas Internos aseguran el cumplimiento del nivel de seguridad requerido por el reglamento para la utilización de datos reales en pruebas.