INDRA SISTEMAS

POLÍTICA DE CERTIFICACIÓN DEL CERTIFICADO PERSONAL DE AUTENTICACIÓN

PKI Interna de Indra (IDR-PKI)

Código: **IDR-PKI-CP01**

Versión: **0.0.1**

Fecha: **25/05/2017**

Control documental

Documento / Fichero	
Título: **Política de Certificación del Certificado Personal de Autenticación**	Nombre fichero:
Código: **IDR-PKI-CP01**	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**

Índice

1. INTRODUCCIÓN 9

1.1. Objetivo y alcance del documento 9

1.2. Documentos relacionados 9

2. ENTIDADES Y PERSONAS INTERVINIENTES 10

2.1. AUTORIDADES DE CERTIFICACIÓN 10

2.2. AUTORIDADES DE REGISTRO 10

2.3. AUTORIDAD DE VALIDACIÓN 10

2.4. TITULARES DE LOS CERTIFICADOS 11

2.5. TERCEROS ACEPTANTES 11

2.6. OTROS AFECTADOS 11

3. USO DE LOS CERTIFICADOS 12

3.1. USOS APROPIADOS DE LOS CERTIFICADOS 12

3.2. LIMITACIONES Y RESTRICCIONES EN EL USO DE LOS CERTIFICADOS 12

3.3. ADMINISTRACIÓN DE LAS POLÍTICAS 12

3.3.1. INDRA como titular de INDRAPKI 12

3.3.2. Determinación de la adecuación de la DPC de una AC externa a las Políticas de Certificación de INDRAPKI 12

3.3.3. Procedimientos de Aprobación de esta PC 12

3.4. DEFINICIONES Y ACRÓNIMOS 13

3.4.1. Definiciones 13

3.4.2. Acrónimos 13

4. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN 15

4.1. REPOSITORIOS 15

4.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN 15

4.3. TEMPORALIDAD O FRECUENCIA DE PUBLICACIÓN 16

4.4. CONTROLES DE ACCESO A LOS REPOSITORIOS 16

5. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS 17

5.1. NOMBRES 17

5.1.1. Tipos de nombres 17

5.1.2. Necesidad de que los nombres sean significativos 17

5.1.3. Reglas para interpretar varios formatos de nombres 17

5.1.4. Unicidad de los nombres 17

5.1.5. Procedimientos de resolución de conflictos sobre nombres 17

5.1.6. Reconocimiento, autenticación y papel de las marcas registradas 18

5.2. VALIDACIÓN DE LA IDENTIDAD INICIAL 18
5.2.1. Medio de prueba de posesión de la clave privada 18
5.2.2. Autenticación de la identidad de una persona jurídica 18
5.2.3. Autenticación de la identidad de una persona física 18
5.2.4. Información no verificada sobre el solicitante 18
5.2.5. Comprobación de las facultades de representación 18
5.2.6. Criterios para operar con AC externas 18
5.3. IDENTIFICACIÓN Y AUTENTICACIÓN EN LAS PETICIONES DE RENOVACIÓN DE CLAVES 19
5.3.1. Identificación y autenticación por una renovación de claves de rutina 19
5.3.2. Identificación y autenticación por una renovación de claves tras una revocación 19

6. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 20

6.1. SOLICITUD DE CERTIFICADOS 20
6.1.1. Quién puede efectuar una solicitud 20
6.2. EMISIÓN DE CERTIFICADOS 21
6.2.1. Emisión de Certificados 21
6.2.2. Notificación al solicitante de la emisión por la AC del certificado 21
6.3. PAR DE CLAVES Y USO DEL CERTIFICADO 21
6.3.1. Uso de la clave privada y del certificado por el titular 21
6.3.2. Uso de la clave pública y del certificado por los terceros aceptantes 21
6.4. RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES 22
6.4.1. Circunstancias para la renovación de certificados sin cambio de claves 22
6.5. RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES 22
6.5.1. Circunstancias para una renovación con cambio claves de un certificado 22
6.5.2. Quién puede pedir la renovación de un certificado 22
6.5.3. Tramitación de las peticiones de renovación de certificados con cambio de claves 22
6.5.4. Notificación de la emisión de un nuevo certificado al titular 23
6.5.5. Forma de aceptación del certificado con las claves cambiadas 23
6.5.6. Publicación del certificado con las nuevas claves por la AC 23
6.5.7. Notificación de la emisión del certificado por la AC a otras Autoridades 23
6.6. MODIFICACIÓN DE CERTIFICADOS 23
6.6.1. Circunstancias para la modificación de un certificado 23
6.7. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 23
6.7.1. Circunstancias para la revocación 23
6.7.2. Quien puede solicitar la revocación 24
6.7.3. Procedimiento de solicitud de revocación 24
6.7.4. Periodo de gracia de la solicitud de revocación 25
6.7.5. Plazo en el que la AC debe resolver la solicitud de revocación 25
6.7.6. Requisitos de verificación de las revocaciones por los terceros aceptantes 25
6.7.7. Frecuencia de emisión de CRLs 25
6.7.8. Tiempo máximo entre la generación y la publicación de las CRL 25
6.7.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados 25

6.7.10. Otras formas de divulgación de información de revocación disponibles 26
6.7.11. Requisitos especiales de renovación de claves comprometidas 26
6.7.12. Causas para la suspensión 26
6.7.13. Quién puede solicitar la suspensión 26
6.7.14. Procedimiento para la solicitud de suspensión 26
6.7.15. Límites del periodo de suspensión 26
6.8. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS 27
6.8.1. Características operativas 27
6.8.2. Disponibilidad del servicio 27
6.8.3. Características adicionales 27
6.9. EXTINCIÓN DE LA VALIDEZ DE UN CERTIFICADO 27
6.10. CUSTODIA Y RECUPERACIÓN DE CLAVES 27
6.10.1. Prácticas y políticas de custodia y recuperación de claves 27
6.10.2. Prácticas y políticas de protección y recuperación de la clave de sesión 27

7. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES 28

7.1. CONTROLES FÍSICOS 28
7.1.1. Ubicación física y construcción 28
7.1.2. Acceso físico 28
7.1.3. Alimentación eléctrica y aire acondicionado 28
7.1.4. Exposición al agua 28
7.1.5. Protección y prevención de incendios 28
7.1.6. Sistema de almacenamiento 28
7.1.7. Eliminación de residuos 28
7.1.8. Copias de seguridad fuera de las instalaciones 29
7.2. CONTROLES DE PROCEDIMIENTO 29
7.2.1. Roles responsables del control y gestión de la PKI 29
7.2.2. Número de personas requeridas por tarea 29
7.2.3. Identificación y autenticación para cada usuario 29
7.2.4. Roles que requieren segregación de funciones 29
7.3. CONTROLES DE PERSONAL 29
7.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales 29
7.3.2. Procedimientos de comprobación de antecedentes 29
7.3.3. Requerimientos de formación 29
7.3.4. Requerimientos y frecuencia de actualización de la formación 30
7.3.5. Frecuencia y secuencia de rotación de tareas 30
7.3.6. Sanciones por acciones no autorizadas 30
7.3.7. Requisitos de contratación de terceros 30
7.3.8. Documentación proporcionada al personal 30
7.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD 30
7.4.1. Tipos de eventos registrados 30
7.4.2. Frecuencia de procesado de registros de auditoría 30
7.4.3. Periodo de conservación de los registros de auditoría 30
7.4.4. Protección de los registros de auditoría 30

7.4.5. Procedimientos de respaldo de los registros de auditoría 31
7.4.6. Sistema de recogida de información de auditoría (interno vs externo) 31
7.4.7. Notificación al sujeto causa del evento 31
7.4.8. 5.4.8. Análisis de vulnerabilidades 31
7.5. ARCHIVO DE REGISTROS 31
7.5.1. Tipo de eventos archivados 31
7.5.2. Periodo de conservación de registros 31
7.5.3. Protección del archivo 31
7.5.4. Procedimientos de copia de respaldo del archivo 31
7.5.5. Requerimientos para el sellado de tiempo de los registros 32
7.5.6. Sistema de archivo de información de auditoría (interno vs externo) 32
7.5.7. Procedimientos para obtener y verificar información archivada 32
7.6. CAMBIO DE CLAVES DE UNA AC 32
7.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O CATÁSTROFE 32
7.7.1. Procedimientos de gestión de incidentes y compromisos 32
7.7.2. Alteración de los recursos hardware, software y/o datos 32
7.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad 32
7.7.4. Instalación después de un desastre natural u otro tipo de catástrofe 32
7.8. CESE DE UNA AC O AR 33
7.8.1. Autoridad de Certificación 33
7.8.2. Autoridad de Registro 33

8. CONTROLES DE SEGURIDAD TÉCNICA 34

8.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 34
8.1.1. Generación del par de claves 34
8.1.2. Entrega de la clave privada al titular 34
8.1.3. Entrega de la clave publica al emisor del certificado 34
8.1.4. Entrega de la clave pública de la AC a los terceros aceptantes 34
8.1.5. Tamaño de las claves 34
8.1.6. Parámetros de generación de la clave pública y verificación de la calidad 34
8.1.7. Fines del uso de la clave (campo KeyUsage de X.509 v3) 35
8.2. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 35
8.2.1. Archivo de la clave pública 35
8.2.2. Periodos operativos de los certificados y periodo de uso para el par de claves 35
8.3. DATOS DE ACTIVACIÓN 35
8.3.1. Generación e instalación de los datos de activación 35
8.3.2. Protección de los datos de activación 35
8.3.3. Otros aspectos de los datos de activación 36
8.4. CONTROLES DE SEGURIDAD INFORMÁTICA 36
8.4.1. Requerimientos técnicos de seguridad específicos 36
8.4.2. Evaluación de la seguridad informática 36
8.5. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 36
8.5.1. Controles de desarrollo de sistemas 36

8.5.2. Controles de gestión de seguridad 36
8.5.3. Controles de seguridad del ciclo de vida 36
8.6. CONTROLES DE SEGURIDAD DE LA RED 36
8.7. SELLADO DE TIEMPO 36

9. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP 37

9.1. PERFIL DE CERTIFICADO 37
9.1.1. Número de versión 37
9.1.2. Perfil del certificado 37

10. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES 39

10.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD ... 39
10.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR 39
10.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA 39
10.4. ASPECTOS CUBIERTOS POR LOS CONTROLES 39
10.5. ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS 39
10.6. COMUNICACIÓN DE RESULTADOS 39

11. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD 40

11.1. TARIFAS 40
11.1.1. Tarifas de emisión de certificado o renovación 40
11.1.2. Tarifas de acceso a los certificados 40
11.1.3. Tarifas de acceso a la información de estado o revocación 40
11.1.4. Tarifas de otros servicios tales como información de políticas 40
11.1.5. Política de reembolso 40
11.2. RESPONSABILIDADES ECONÓMICAS 40
11.2.1. Cobertura asegurada 40
11.2.2. Otros activos 41
11.2.3. Cobertura de seguro u otras garantías para los terceros aceptantes 41
11.3. CONFIDENCIALIDAD DE LA INFORMACIÓN 41
11.3.1. Ámbito de la información confidencial 41
11.3.2. Información no confidencial 41
11.3.3. Deber de secreto profesional 41
11.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL 41
11.4.1. Política de protección de datos de carácter personal 41
11.4.2. Información tratada como privada 41
11.4.3. Información no calificada como privada 41
11.4.4. Responsabilidad de la protección de los datos de carácter personal 42
11.4.5. Comunicación y consentimiento para usar datos de carácter personal 42
11.4.6. Revelación en el marco de un proceso judicial 42
11.4.7. Otras circunstancias de publicación de información 42
11.5. DERECHOS DE PROPIEDAD INTELECTUAL 42

11.6. OBLIGACIONES Y RESPONSABILIDADES 42
11.6.1. Obligaciones y responsabilidades de la AC 42
11.6.2. Obligaciones de la AR 42
11.6.3. Obligaciones de los titulares de los certificados 43
11.6.4. Obligaciones de los terceros aceptantes 43
11.6.5. Obligaciones de otros participantes 43
11.7. LIMITACIONES DE RESPONSABILIDADES 43
11.8. DELIMITACIÓN DE RESPONSABILIDADES 43
11.9. LIMITACIONES DE PÉRDIDAS 43
11.10. PERIODO DE VALIDEZ 43
11.10.1. Plazo 43
11.10.2. Sustitución y derogación de la PC 44
11.10.3. Efectos de la finalización 44
11.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES 44
11.12. PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES 44
11.12.1. Procedimiento para los cambios 44
11.12.2. Periodo y mecanismo de notificación 44
11.12.3. Circunstancias en las que el OID debe ser cambiado 44
11.13. RECLAMACIONES Y JURISDICCIÓN 44
11.14. NORMATIVA APLICABLE 45
11.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE 45
11.16. ESTIPULACIONES DIVERSAS 45
11.16.1. Cláusula de aceptación completa 45
11.16.2. Independencia 45
11.16.3. Resolución por la vía judicial 45
11.17. OTRAS ESTIPULACIONES 45

12. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 46

12.1. RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS 46
12.2. CREACIÓN DEL FICHERO E INSCRIPCIÓN REGISTRAL 46
12.3. DOCUMENTO DE SEGURIDAD LOPD 46

1. INTRODUCCIÓN

1.1. Objetivo y alcance del documento

Este documento recoge la Política de Certificación (PC) que rige los Certificados Personales de Autenticación emitidos por la Autoridad de Certificación Corporativa de la Infraestructura de Clave Pública (en adelante PKI) de Indra (desde ahora INDRAPKI).

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de un certificado en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

En esta PC se detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI de Indra (INDRAPKI), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

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 normativa española en la materia.

La PC incluye todas las actividades encaminadas a la gestión de los certificados de autenticación en su ciclo de vida, y sirve de guía de la relación entre la AC Corporativa V2 y sus usuarios. En consecuencia, todas las partes involucradas tienen la obligación de conocer la PC y ajustar su actividad a lo dispuesto en la misma.

Esta PC 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.

1.2. Documentos relacionados

Documentos relacionados a la presente política de certificación:

- Declaración de Prácticas de Certificación

2. ENTIDADES Y PERSONAS INTERVINIENTES

2.1. AUTORIDADES DE CERTIFICACIÓN

Esta PC hace referencia a los certificados de autenticación emitidos por la AC Corporativa V2 de INDRAPKI. Sus datos más relevantes son:

Tabla 1 Datos de la AC Corporativa V2

Nombre distintivo	CN=INDRA AC CORPORATIVA V2, OU=PKI, O=Indra, C=ES
Número de serie	13 75 ec ce 44 ba 87 12 57 0b ac 46 dd cb 7d 96
Nombre distintivo del emisor	CN=INDRA AC RAIZ V2, OU=PKI, O=Indra, C=ES
Fecha de emisión	lunes, 11 de abril de 2016 15:53:10
Fecha de expiración	viernes, 11 de abril de 2031 15:53:10
Longitud de clave RSA	2048 Bits
Huella digital (SHA-1)	fb 96 7c 1d 6c 11 98 06 63 39 b3 17 f8 98 58 ed 00 a4 67 89
URL de publicación del certificado	**https://pki.indraweb.net/certs/indra-corp-v2.crt**
URL de publicación de la CRL	**https://pki.indraweb.net/crls/indra-corp-v2.crl**

2.2. AUTORIDADES DE REGISTRO

La emisión de certificados de autenticación a través de la aplicación “Certificados” disponible en la INDRAWEB en el Menú “Mi Trabajo – Herramientas”.

2.3. AUTORIDAD DE VALIDACIÓN

Una Autoridad de Validación (AV) tiene como función la comprobación del estado de los certificados emitidos por INDRAPKI, mediante el protocolo *Online Certificate Status Protocol* (OCSP), que determina el estado actual de un certificado electrónico a solicitud de un Tercero Aceptante sin requerir el acceso a listas de certificados revocados por éstas.

Este mecanismo de validación es complementario a la publicación de las listas de certificados revocados (CRL).

Actualmente INDRAPKI no dispone de Autoridad de Validación.

2.4. TITULARES DE LOS CERTIFICADOS

Se define Titular de acuerdo con la Declaración de Prácticas de Certificación de INDRAPKI.

Los tipos de personas que pueden ser titulares de certificados de autenticación personales de la AC Corporativa V2 se restringen a los recogidos en el siguiente cuadro:

Tabla 2 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

2.5. TERCEROS ACEPTANTES

Como Terceros Aceptantes se entiende a aquellos que hagan uso de los certificados para identificar a las personas titulares de certificados de autenticación de la AC Corporativa V2 de INDRAPKI.

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.

Administradores de Usuarios: personas que dentro de Indra gestionan las peticiones de certificados personales y verifican su correcta obtención.

3. USO DE LOS CERTIFICADOS

3.1. USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados regulados por esta PC se utilizarán para la **autenticación de personas frente a los Sistemas de Información de Indra**.

3.2. LIMITACIONES Y RESTRICCIONES EN EL USO DE LOS CERTIFICADOS

Cualquier uso no incluido en el apartado anterior queda excluido.

3.3. ADMINISTRACIÓN DE LAS POLÍTICAS

3.3.1. INDRA como titular de INDRAPKI

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

Según lo especificado en la DPC de INDRAPKI.

3.3.3. 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 PC.

La AAP también se encarga de aprobar y autorizar las modificaciones del documento.

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

AV: Autoridad de Validación.

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 3 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?objectclass=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

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

4.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

4.3. TEMPORALIDAD O FRECUENCIA DE PUBLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

4.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

5. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS

5.1. NOMBRES

5.1.1. Tipos de nombres

Los certificados emitidos por INDRAPKI contienen el nombre distintivo (D*istinguished Name* o DN) X.500 del emisor y el destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

El atributo CN (*Common Name*) del DN contiene el código o identificador del usuario en los sistemas internos de Indra (cuenta del directorio activo). Este identificador es único.

Adicionalmente se utilizan los siguientes campos:

- givenName = Nombre del usuario (OID**:** 2.5.4.42)
- surName = Apellidos del usuario (OID**:** 2.5.4.4)

El resto de atributos del DN tendrá los siguientes valores fijos:

- OU=Personas, O=Indra, C=ES

5.1.2. Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos de los certificados han de ser significativos y se aplicarán las reglas establecidas en el apartado anterior para ello.

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

El DN de los certificados no puede estar repetido. La utilización del código único de usuario garantiza la unicidad del DN.

5.1.5. Procedimientos de resolución de conflictos sobre nombres

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

El par de claves de los certificados de autenticación personal los generará la AC Corporativa V2, con lo que no aplica este apartado.

5.2.2. Autenticación de la identidad de una persona jurídica

No está contemplado que los certificados de autenticación personales sean emitidos para personas jurídicas ajenas a INDRA, por lo que no procede definir un procedimiento de identificación de las mismas.

5.2.3. Autenticación de la identidad de una persona física

La autenticación inicial de la identidad de un individuo es presencial. El solicitante se ha de presentar ante su Administrador de usuarios debidamente identificado mediante su tarjeta actual de empleado o subcontratado.

5.2.4. Información no verificada sobre el solicitante

Toda la información recabada en el apartado anterior ha de ser verificada.

5.2.5. Comprobación de las facultades de representación

El solicitante del certificado de autenticación actúa en nombre propio por ser empleado, colaborador o subcontratado de Indra, por lo que no aplica este apartado.

5.2.6. Criterios para operar con AC externas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Solo se contempla la autenticación de la identidad de un individuo de forma presencial, antes el Administrador de Usuarios. Este método será utilizado tanto en la emisión inicial del certificado como en el caso de renovación del anterior.

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

El proceso de identificación individual será presencial y con los mismos criterios que en una renovación de rutina.

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

En este capítulo se recogen los requisitos operacionales para el ciclo de vida de los certificados de autenticación personal emitidos por la AC Corporativa v2. Aunque estos certificados se van a almacenar en tarjetas criptográficas, no es objeto de esta Política de Certificación regular la gestión de dichas tarjetas, por lo que siempre se parte de que el solicitante del certificado ha obtenido previamente su tarjeta criptográfica.

Por otro lado, en este capítulo se van a emplear algunas ilustraciones para facilitar su comprensión. En el caso de que existiera alguna diferencia o discrepancia entre lo recogido en el texto y lo recogido en las ilustraciones prevalecería siempre el texto, dado el carácter necesariamente sintético de las ilustraciones.

6.1. SOLICITUD DE CERTIFICADOS

6.1.1. Quién puede efectuar una solicitud

La petición de un certificado de autenticación personal está referida a dos tipos de colectivos:

- **Empleados**: se entiende que la petición se efectúa automáticamente por el hecho de su incorporación a la plantilla de Indra. Una vez que el empleado se encuentre en posesión de la tarjeta criptográfica corporativa, éste recibirá una citación para acudir al servicio de registro de la PKI, donde será generado el certificado de autenticación.
- **Colaboradores y Subcontratados**: la petición la debe hacer el Departamento en el que estén asignados en función de su necesidad de acceder a los Sistemas de Información. El colaborador o subcontratado deberá acudir, con su tarjeta criptográfica corporativa, al servicio de registro de la PKI, donde será generado el certificado de autenticación.

La solicitud del certificado no implica su obtención si el solicitante no cumple los requisitos establecidos en la DPC y en esta PC para certificados de autenticación. El Administrador de la PKI podrá recabar del solicitante la documentación que considere oportuna.

6.2. EMISIÓN DE CERTIFICADOS

6.2.1. Emisión de Certificados

El usuario solicita puede solicitar sus certificados a través de la aplicación "Certificados" disponible en la INDRAWEB en el Menú "Mi Trabajo – Herramientas". Antes de la emisión el usuario debe elegir la contraseña con la que va a proteger los certificados.

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

Por norma general, el usuario recibe el certificado unos 5 minutos después de realizar la solicitud. El usuario recibe un correo con los certificados.

6.3. PAR DE CLAVES Y USO DEL CERTIFICADO

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

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo 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 de uso establecidas en la DPC y PC y sólo para lo que éstas establezcan.

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

Los certificados de autenticación regulados por esta PC sólo pueden ser utilizados para prestar los siguientes servicios de seguridad:

- Autenticación frente a los sistemas de información de Indra que demanden la comprobación de la identidad del titular mediante certificado electrónico.

6.3.2. 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 establece esta PC y de acuerdo 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 la DPC y en esta PC. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos.

6.4. RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

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

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

6.5. RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

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

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

- Expiración del periodo de validez.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de las mismas.
- Cambio de formato.

Todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves.

6.5.2. Quién puede pedir la renovación de un certificado

La renovación la debe solicitar el titular del certificado.

6.5.3. 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 identificación y autenticación para la renovación de un certificado de autenticación se realizará de forma presencial en los puestos de registro que se establezcan de igual forma que en el caso de la emisión inicial.

Si alguna de las condiciones establecidas en esta PC han 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 lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que INDRAPKI especifica a tal efecto. Sólo se puede solicitar la renovación de un certificado dentro de sus últimos 60 días de vigencia.
- 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 servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

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

Se notificará mediante correo electrónico.

6.5.5. Forma de aceptación del certificado con las claves cambiadas

En el caso de las renovaciones presenciales ha de firmar la aceptación al Administrador de Usuarios (copia para el interesado y copia para la empresa).

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

El certificado de autenticación quedará almacenado exclusivamente en el repositorio interno de INDRAPKI, no estando accesible a través de ningún repositorio público.

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

No estipulado.

6.6. MODIFICACIÓN DE CERTIFICADOS

6.6.1. Circunstancias para la modificación de un certificado

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

6.7. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

6.7.1. 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.

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

Un certificado de Autenticación personal puede ser revocado por:

- 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 contenidos en el documento de Aceptación de las condiciones de uso de los certificados personales, en la DPC o en la presente PC.
- El titular de un certificado deja de pertenecer al grupo, circunstancia que le facultaba para la posesión del certificado.
- Emisión defectuosa de un certificado debido a que:
  - No se ha cumplido un requisito material para la emisión del certificado.
  - La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
  - 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 titular o por 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 PC o en la DPC.

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.

6.7.2. 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.

Asimismo, los titulares de certificados también podrán solicitar la revocación de sus certificados, debiendo solicitar la revocación de acuerdo con las condiciones especificadas en el 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.

6.7.3. Procedimiento de solicitud de revocación

El titular o persona que solicite la revocación la debe presentar ante un administrador de usuarios, identificándose indicando la causa de la solicitud.

El Administrador de usuarios tramitará siempre las solicitudes de revocación de aquellos titulares que tenga asignados. La solicitud se realiza a través de una Autoridad de Registro.

Además de este procedimiento ordinario, los Custodios y Administradores de la PKI podrán revocar de modo inmediato cualquier certificado caso de que llegue a su conocimiento la existencia de alguna causa que motive la revocación.

6.7.4. 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.

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

La solicitud de revocación de un certificado de autenticación debe ser atendida con la máxima celeridad, sin que en ningún caso su tratamiento pueda ser superior a 24 horas.

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

La verificación de las revocaciones es obligatoria para cada uso de los certificados de Autenticación.

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.

Para los certificados de autenticación el procedimiento ordinario de comprobación de la validez de un certificado será la consulta a la CRL del repositorio de INDRAPKI.

6.7.7. Frecuencia de emisión de CRLs

INDRAPKI publicará una nueva CRL en su repositorio en el momento 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.

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

El tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio es de 6 horas.

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

INDRAPKI proporciona un servidor web donde publica las CRLs al comienzo del presente documento, para la verificación del estado de los certificados que emite.

6.7.10. Otras formas de divulgación de información de revocación disponibles

No estipulado.

6.7.11. 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.

6.7.12. Causas para la suspensión

La suspensión de certificados se podrá dar 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.
- 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.
- Resolución judicial o administrativa que lo ordene.

6.7.13. Quién puede solicitar la suspensión

La solicitud la puede iniciar el titular del certificado.

6.7.14. Procedimiento para la solicitud de suspensión

La solicitud de suspensión la tramitará el Administrador de Usuarios a través de una Autoridad de Registro. Por el mismo método se solicitará el levantamiento de la suspensión cuando proceda éste.

En cualquier caso, se le comunicará al titular del certificado tanto el comienzo de la suspensión como su fin por correo electrónico.

6.7.15. Límites del periodo de suspensión

Por defecto INDRAPKI suspenderá los certificados de forma provisional por un plazo máximo de 1 año, 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 ese mismos casos de caducidad o revocación.

6.8. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

6.8.1. Características operativas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

6.8.2. Disponibilidad del servicio

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

6.8.3. Características adicionales

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

6.9. 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.

6.10. CUSTODIA Y RECUPERACIÓN DE CLAVES

6.10.1. Prácticas y políticas de custodia y recuperación de claves

No se efectúa archivo de la clave privada de autenticación.

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

No estipulado.

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

7.1. CONTROLES FÍSICOS

7.1.1. Ubicación física y construcción

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.2. Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.3. Alimentación eléctrica y aire acondicionado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.4. Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.5. Protección y prevención de incendios

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.6. Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.7. Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.1.8. Copias de seguridad fuera de las instalaciones

No aplicable

7.2. CONTROLES DE PROCEDIMIENTO

7.2.1. Roles responsables del control y gestión de la PKI

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.2.2. Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.2.3. Identificación y autenticación para cada usuario

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.2.4. Roles que requieren segregación de funciones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3. CONTROLES DE PERSONAL

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.4. Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.6. Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.7. Requisitos de contratación de terceros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

7.4.1. Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4.2. Frecuencia de procesado de registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4.3. Periodo de conservación de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4.4. Protección de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4.5. Procedimientos de respaldo de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4.7. Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.4.8. 5.4.8. Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.5. ARCHIVO DE REGISTROS

7.5.1. Tipo de eventos archivados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.5.2. Periodo de conservación de registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.5.3. Protección del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.5.4. Procedimientos de copia de respaldo del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.5.5. Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.5.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.6. CAMBIO DE CLAVES DE UNA AC

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

7.7.1. Procedimientos de gestión de incidentes y compromisos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.8. CESE DE UNA AC O AR

7.8.1. Autoridad de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

7.8.2. Autoridad de Registro

No estipulado

8. CONTROLES DE SEGURIDAD TÉCNICA

8.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

8.1.1. Generación del par de claves

Las claves para los certificados de Autenticación emitidos por la AC Corporativa V2 se generan en el interior de la tarjeta criptográfica corporativa, con certificación ITSEC E4.

8.1.2. Entrega de la clave privada al titular

La clave privada ha sido generada por la Autoridad de Registro Presencial en la tarjeta criptográfica corporativa, por lo no procede esta entrega.

8.1.3. Entrega de la clave publica al emisor del certificado

La clave pública ha sido generada por la Autoridad de Registro Presencial en la tarjeta criptográfica corporativa, por lo que no procede esta entrega.

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

La clave pública de la AC Corporativa V2 está incluida en el certificado de dicha AC.

El certificado de la AC Corporativa V2 no viene incluido en el certificado generado para el titular.

El certificado de la AC Corporativa V2 debe ser obtenido del repositorio especificado en este documento donde queda a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de comprobación.

8.1.5. Tamaño de las claves

El tamaño mínimo de las claves de los certificados de autenticación es de 1024 bits.

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

La clave pública de los certificados de autenticación está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA.

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

La clave definida por la presente política, y por consiguiente el certificado asociado, se utilizará para la verificación de la identidad del titular del certificado frente a los sistemas de información de Indra.

A tal efecto, en los campos '*Key Usage*' y '*Extended Key Usage*' del certificado se han incluido los siguientes usos:

Key Usage:

- Digital Signature.
- Key Agreement
- Key Encipherment

Extended Key Usage:

- clientAuth.
- smartCardLogon
- ipSecUser
- anyExtendedKeyUsage

8.2. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

8.2.1. Archivo de la clave pública

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

El certificado de autenticación y su par de claves asociados tiene un periodo de uso de 2 años, si bien en el momento de su emisión la AC Corporativa V2 puede establecer periodos inferiores.

8.3. DATOS DE ACTIVACIÓN

8.3.1. Generación e instalación de los datos de activación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.3.2. Protección de los datos de activación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.3.3. Otros aspectos de los datos de activación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.4. CONTROLES DE SEGURIDAD INFORMÁTICA

8.4.1. Requerimientos técnicos de seguridad específicos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.4.2. Evaluación de la seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.5. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

8.5.1. Controles de desarrollo de sistemas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.5.2. Controles de gestión de seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.5.3. Controles de seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.6. CONTROLES DE SEGURIDAD DE LA RED

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

8.7. SELLADO DE TIEMPO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

9. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

9.1. PERFIL DE CERTIFICADO

9.1.1. Número de versión

Los certificados de autenticación personales emitidos por la AC Corporativa V2 utilizan el estándar X.509 versión 3 (X.509 v3)

9.1.2. Perfil del certificado

El perfil del certificado es el siguiente:

Tabla 4 Perfil de certificado de autenticación

Campo	Contenido Propuesto	Crítica
1. Versión	v3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=INDRA AC CORPORATIVA V2, OU=PKI, O=Indra, C=ES	
5. Validity	2 años	
6. Subject	CN=*SAMAccountName* givenName=Nombre sn=Apellidos OU=Personas O=Indra C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 1024 bits	
8. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.8173.2.2.6	
URL CPS	*[URL CPS]*	
9. Policy Mappings	No utilizado	

10. Subject Alternate Names	UPN (User´s Principal Name de Windows) Email RFC822 (opcional) 1.3.6.1.4.1.8173.2.3.1 Nombre 1.3.6.1.4.1.8173.2.3.11 Apellidos 1.3.6.1.4.1.8173.2.3.4 Número de empleado 1.3.6.1.4.1.8173.2.3.5 SAMAccountName	
11. Issuer Alternate Names	No utilizado	
11. KeyUsage	Digital Signature Key Agreement	SI
12. extKeyUsage	clientAuth, smartCardLogon.	NO
13. Subject Key Identifier	SHA-1 hash de la clave pública	NO
14. Authority Key Identifier	Se utilizará	
KeyIdentifier	SHA-1 hash de la clave pública del emisor	
AuthorityCertIssuer	No utilizado	
AuthorityCertSerialNumber	No utilizado	
15. Issuer Alternate Names	No utilizado	
16. Subject Directory Attributes	No utilizado	
17. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	Ninguno	
18. CRLDistributionPoints	(1) HTTP: *[HTTP URI CRL]* (2) Directorio Activo: *[AD URI CRL]*	
19. Auth. Information Access	No utilizado	

10. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

10.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

10.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

10.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

10.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

10.6. COMUNICACIÓN DE RESULTADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

11.1. TARIFAS

11.1.1. Tarifas de emisión de certificado o renovación

No se aplica ninguna tarifa sobre la emisión o renovación de certificados bajo el amparo de la presente Política de Certificación.

11.1.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos bajo esta Política, dada su naturaleza publica, es libre y gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

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

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

11.1.4. Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

11.1.5. Política de reembolso

Al no existir ninguna tarifa de aplicación para esta Política de Certificación no es necesaria ninguna política de reintegros.

11.2. RESPONSABILIDADES ECONÓMICAS

11.2.1. Cobertura asegurada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.2.2. Otros activos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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.

11.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

11.3.1. Ámbito de la información confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.3.2. Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.3.3. Deber de secreto profesional

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

11.4.1. Política de protección de datos de carácter personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.4.2. Información tratada como privada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.4.3. Información no calificada como privada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.4.5. Comunicación y consentimiento para usar datos de carácter personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.4.6. Revelación en el marco de un proceso judicial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.4.7. Otras circunstancias de publicación de información

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.5. DERECHOS DE PROPIEDAD INTELECTUAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.6. OBLIGACIONES Y RESPONSABILIDADES

11.6.1. Obligaciones y responsabilidades de la AC

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

La Autoridad de Certificación Corporativa de INDRAPKI actuará relacionando una determinada clave pública con su titular mediante la emisión de un certificado de autenticación, todo ello de conformidad con los términos de esta PC y de la DPC.

Los servicios prestados por la AC en el contexto de esta PC son los servicios de emisión, renovación y revocación de certificados de autenticación personales, a los que se accede mediante los Puestos de Administración remotos de la AC desplegados a tal efecto.

11.6.2. Obligaciones de la AR

No estipulado.

11.6.3. Obligaciones de los titulares de los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.6.4. Obligaciones de los terceros aceptantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.6.5. Obligaciones de otros participantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.7. LIMITACIONES DE RESPONSABILIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.8. DELIMITACIÓN DE RESPONSABILIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.9. LIMITACIONES DE PÉRDIDAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.10. PERIODO DE VALIDEZ

11.10.1. Plazo

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

Esta PC 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 Corporativa, ocasión en que obligatoriamente se emitirá una nueva versión.

11.10.2. Sustitución y derogación de la PC

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

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

11.10.3. Efectos de la finalización

Las obligaciones y restricciones que establece esta PC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de INDRAPKI, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

11.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.12. PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES

11.12.1. Procedimiento para los cambios

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.12.2. Periodo y mecanismo de notificación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.12.3. Circunstancias en las que el OID debe ser cambiado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.13. RECLAMACIONES Y JURISDICCIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.14. NORMATIVA APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.16. ESTIPULACIONES DIVERSAS

11.16.1. Cláusula de aceptación completa

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

11.16.2. Independencia

En el caso que una o más estipulaciones de esta PC sea o llegase a ser inválida, nula, o inexigible legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la PC careciera ésta de toda eficacia jurídica.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

12.2. CREACIÓN DEL FICHERO E INSCRIPCIÓN REGISTRAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.

12.3. DOCUMENTO DE SEGURIDAD LOPD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de INDRAPKI.