NORMAS

PARLAMENTO DE ANDALUCÍA

Normas administrativas, económicas y organizativas

XII Legislatura

RELACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL PARLAMENTO DE ANDALUCÍA

Número de expediente: 12-26/ACME-000003

Acuerdo de la Mesa del Parlamento de Andalucía, de 11 de marzo de 2026

Publicado en *BOPA* núm. 885, de 12 de marzo de 2026

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL PARLAMENTO DE ANDALUCÍA

ÍNDICE

INFORMACIÓN PRELIMINAR 3

Introducción 3

Objeto 3

Ámbito de aplicación 3

Marco normativo 4

Términos y definiciones 4

COMPONENTES 6

Tipos de certificados 6

Autoridades de certificación 6

Autoridad de registro 7

Autoridad de validación 8

Usuarios 9

PROCEDIMIENTOS 10

Generación de claves y certificados de AC 10

Generación de certificados de usuario para firma automatizada 11

Renovación de certificados 12

Revocación de certificados 12

Suspensión de certificados 13

Publicación de CRL 13

Autorización de firma 14

Reemisión por cambio de grupo parlamentario 14

Terminación de la AC 14

Gestión de incidentes 14

MEDIDAS DE SEGURIDAD 15

PERFIL TÉCNICO 16

PUBLICIDAD 18

REVISIÓN Y APROBACIÓN 18

INFORMACIÓN PRELIMINAR

INTRODUCCIÓN

El Parlamento de Andalucía (PA) tiene una dilatada experiencia en la utilización de certificados electrónicos para la identificación y firma electrónica, disponiendo de acreditación para registrar certificados electrónicos de persona física y de empleado público de la Fábrica Nacional de Moneda y Timbre y Real Casa de la Moneda (FNMT-RCM).

No obstante, la transformación digital que lleva a cabo esta institución requiere implementar sistemas de información que proporcionen una flexibilidad en la realización de firmas electrónicas con la misma validez que las actuales, de modo que el personal de los grupos parlamentarios pueda solicitar la firma electrónica de documentos, previa autorización de los diputados y diputadas, dentro del propio sistema de gestión, validación, firma y presentación de iniciativas. Para evitar riesgos innecesarios, estas firmas generadas por sistemas internos, únicamente para el uso en iniciativas parlamentarias o documentos que van a presentarse en el Registro General del Parlamento de Andalucía, no deben tener validez fuera de la institución, por lo que hace falta establecer una infraestructura de clave pública (PKI) interna que permita realizar firmas electrónicas con validez única y exclusivamente en el ámbito de la tramitación de iniciativas dentro de los sistemas de información del propio Parlamento de Andalucía.

OBJETO

Este documento es la declaración de prácticas de certificación (CPS[1]) del Parlamento de Andalucía y tiene como objeto establecer los procedimientos, responsabilidades y obligaciones que rigen el funcionamiento de la PKI interna de la institución (PKI-PA).

ÁMBITO DE APLICACIÓN

Este documento se aplica a todo el personal que opere sobre sistemas de información que empleen certificados emitidos por la PKI-PA o firmas electrónicas realizadas con estos, incluyendo:

Titulares de certificados electrónicos emitidos por la PKI-PA.

Usuarios de documentos con firmas electrónicas realizadas con dichos certificados.

Desarrolladores de aplicaciones que integren servicios de firma o de validación de firmas electrónicas que operen sobre dichos certificados.

Operadores de los sistemas de información sobre los que se implemente la PKI-PA, incluidas las autoridades de certificación, registro y validación.

[1] Certification Practices Statement.

MARCO NORMATIVO

En la elaboración de este documento se ha tenido en cuenta el siguiente marco normativo:

Política de seguridad de la información del Parlamento de Andalucía, que define el marco general de gestión de la seguridad en la institución.

Normas de administración electrónica en el Parlamento de Andalucía, acuerdo de la Mesa del Parlamento en sesión celebrada el 19 de mayo de 2020.

Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Esquema Nacional de Seguridad, aprobado por el Real Decreto 311/2022, de 3 de mayo, que establece los principios y requisitos mínimos de seguridad en el ámbito de la Administración pública (ENS).

Recomendación X.509 (The directory: Public-key and attribute certificate frameworks) de ITU-T, que define el formato estándar de los certificados electrónicos y sus listas de revocación.

Recomendación X.501 (The directory: Models) de ITU-T, que define el formato de los nombres distinguidos con los que expresan los titulares de los certificados electrónicos X.509.

Guía RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) de IETF, que define cómo usar los certificados electrónicos X.509 y sus listas de revocación para asegurar la interoperabilidad en Internet.

Guía RFC 3647 (Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework) de IETF, que establece un marco para la redacción y organización de políticas y declaraciones de prácticas de certificación.

Guía NIST 800-88, que establece buenas prácticas para el borrado seguro de los datos.

TÉRMINOS Y DEFINICIONES

Este documento emplea los términos definidos a continuación:

AC: Autoridad de certificación. Componente de una PKI que emite, revoca y suspende certificados, publicando listas de certificados revocados y suspendidos (CRL).

AKI:[2] Identificador de clave de autoridad. Atributo de los certificados electrónicos que contiene una huella digital de la clave pública de la AC que los emitió. Permite optimizar la localización de certificados durante la validación de estos al evitar tener que comparar claves públicas completas.

AR: Autoridad de registro. Componente de una PKI que verifica las solicitudes de emisión de certificados electrónicos y transmite las verificadas a una AC para la emisión del certificado.

DN:[3] Nombre distinguido. Formato en que se expresa el titular de un certificado electrónico.

[2] Authority Key Identifier

[3] Distinguished Name

CDP:[4] Punto de distribución de contenido. Atributo de los certificados electrónicos a través del que se indican las direcciones URL de las listas de certificados revocados y suspendidos (CRL) por la AC emisora del mismo, con objeto de poder utilizarla para validar ese certificado.

Certificado electrónico: Información firmada electrónicamente por una AC que certifica que una determinada identidad es titular de una cierta clave pública de criptografía asimétrica.

Criptografía asimétrica: La que usa dos claves relacionadas, una privada que se mantiene en secreto y se usa para firmar y descifrar información, y una pública que se comparte y se usa para verificar firmas y cifrar información destinada a su titular.

CRL:[5] Lista de revocación de certificados. Lista publicada por una AC con los números de serie de todos los certificados que ha revocado y de las suspensiones de certificados activas.

CSR:[6] Solicitud de firma de certificado. Información en formato electrónico a través de la que se solicita a una AC la emisión de un certificado electrónico que vincule una cierta clave pública a un determinado titular.

CPS:[7] Declaración de prácticas de certificación; es decir, este documento.

CSIRT-PA:[8] Equipo de respuesta a incidentes del PA.

OCSP:[9] Protocolo de validación online del estado de certificados electrónicos.

Firma electrónica: Información en formato electrónico mediante la que una persona asume la autoría o consentimiento de un contenido electrónico. Este documento hace referencia a su implementación más común, basada en criptografía asimétrica: anexar al contenido a firmar el resultado de cifrar su huella digital con la clave privada del firmante, acompañado del certificado electrónico que contiene la clave pública necesaria para verificar la firma y la vincula con la identidad de su titular. La verificación consiste en comprobar que aplicar un cierto algoritmo de verificación a la clave pública y a la firma del contenido devuelve la huella digital del contenido.

Huella digital (hash): Valor alfanumérico resultante de aplicar a un contenido electrónico un algoritmo criptográfico que devuelve un resultado de tamaño fijo que permite identificar dicho contenido unívocamente y detectar cualquier alteración en él.

PA: Parlamento de Andalucía.

PKI:[10] Infraestructura de clave pública. Infraestructura que permite la emisión, gestión y uso seguro de certificados electrónicos para identificación y firma electrónica mediante criptografía de clave pública.

PKI-PA: Infraestructura de clave pública del Parlamento de Andalucía.

SKI:[11] Identificador de clave de titular. Atributo de los certificados electrónicos que contiene una huella digital de la clave pública del titular del certificado. Permite optimizar la localización de certificados durante la validación de estos, al evitar tener que comparar claves públicas completas.

[4] Content Distribution Point.

[5] Certificate Revocation List.

[6] Certificate Signing Request.

[7] Certification Practices Statement.

[8] Computer Incident Response Team.

[9] Online Certificate Status Protocol.

[10] Private Key Infraestructure.

[11] Subject Key Identifier.

SOC-PA:[12] Centro de operaciones de seguridad del Parlamento de Andalucía. Equipo que se encarga de monitorizar la infraestructura TIC del PA, para alertar de los incidentes y problemas de seguridad que detecte en ella.

COMPONENTES

TIPOS DE CERTIFICADOS

El único tipo de certificado electrónico emitido por la PKI-PA, además de los que son técnicamente necesarios para su funcionamiento interno, es el certificado de usuario para firma automatizada. Se emite para una persona física identificada ante la AR del PA, con objeto de que esta persona autorice expresamente a quienes puedan solicitar firma electrónica en su nombre, a través de sistemas de información del Parlamento, circunscribiéndose la validez de estas firmas únicamente al ámbito de la propia institución.

AUTORIDADES DE CERTIFICACIÓN

Las AC son los componentes de la PKI responsables de emitir los certificados electrónicos; revocarlos, si se compromete la seguridad de la clave privada que tienen asociada; suspenderlos, ante sospecha de compromiso de esta, y levantar la suspensión si se confirma que la sospecha era infundada.

Las AC del PA se organizan en:[13]

AC Raíz: denominada «AC Parlamento de Andalucía», es la base del modelo de confianza de la PKI-PA, ya que el Servicio de Informática configurará todos los equipos que operen sobre esta para confiar en los certificados que emita, incluido su propio certificado de AC raíz, generado por ella misma.

AC intermedias: emiten los certificados de los usuarios. Los equipos de los usuarios de la PKI confían en los certificados emitidos por las AC intermedias porque los certificados que identifican a estas AC están firmados por la AC raíz, en quien confían.

Se dispondrá de una AC intermedia por cada grupo parlamentario, con nombres como «AC Grupo Popular», «AC Grupo Socialista», etc. Así, si se da de baja un grupo o se compromete la seguridad de la clave privada de la AC intermedia de un grupo, será sencillo revocar todos los certificados emitidos por esta sin afectar al resto de grupos. Adicionalmente, se tendrá una «AC diputados no adscritos» para los diputados no adscritos a ningún grupo parlamentario.

El personal que opera las AC tiene las siguientes obligaciones:

1. Realizar sus operaciones de acuerdo con este documento.
2. Proteger sus datos de creación de firma, lo que incluye sus claves privadas.

[12] Security Operations Center – Parlamento de Andalucía.

[13] Adicionalmente, se dispondrá de un juego de AC para pruebas en entornos de preproducción, con nombres equivalentes prefijados de «PRE»: «PRE AC Parlamento de Andalucía», «PRE AC Grupo Mixto», etc.

3. Emitir los certificados que se les soliciten conforme a la política de certificación establecida. Estos certificados deben seguir el formato establecido en el estándar internacional X.509 de ITU-T, deben ser consistentes con la información conocida en el momento de la emisión y han de estar libres de errores de ingreso de datos.

4. Garantizar la confidencialidad en el proceso de generación de datos para la creación de la firma y su eventual entrega al firmante, a través de un procedimiento seguro.

5. Usar sistemas y productos confiables, protegidos contra cualquier alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación.

6. Revocar y suspender los certificados emitidos conforme al procedimiento establecido y transmitir dichas revocaciones y suspensiones a la autoridad de validación, de manera que los usuarios de la PKI puedan consultar en todo momento la validez de los certificados emitidos.

7. Mantener en un repositorio seguro toda la información relativa al funcionamiento de la AC durante un periodo de quince años, asegurándose de que durante ese tiempo siempre se pueda determinar con precisión la fecha y hora en que se emitió, expiró o suspendió cada certificado. Este repositorio podrán leerlo las aplicaciones del PA autorizadas para ello, bajo los mecanismos de control que se establezcan al respecto, pero solo podrán modificarlo las AC y en ningún caso incluirá las claves privadas asociadas a los certificados. Incluirá:

- Certificados emitidos y certificados de AC superiores.
- Listas de revocación de certificados publicadas.
- Políticas y prácticas de certificación.
- Registros de acceso a los sistemas sobre los que se implementa la PKI y de auditoría de las operaciones realizas mediante estos: emisiones, revocaciones y suspensiones de certificados, modificaciones de parámetros de configuración de las AC, etc.

8. Colaborar con las auditorías, lo que incluye proporcionar a los auditores acceso al repositorio de certificados y al resto de documentación sobre el funcionamiento de la AC que sea relevante.

9. Mantener la confidencialidad de la información manejada durante y después de la prestación de los servicios.

No es obligación de las AC del PA supervisar, investigar ni confirmar la exactitud de la información contenida en los certificados tras su emisión. No obstante, podrán revocarlos en caso de recibir información sobre la inexactitud o la inaplicabilidad actual de la información que contengan.

AUTORIDAD DE REGISTRO

La AR es el componente de la PKI responsable de verificar la identidad de los solicitantes de certificados electrónicos, registrar evidencias de ello, pasar a las AC las solicitudes de firma de certificados electrónicos una vez validadas y entregar a los solicitantes los certificados que les emitan las AC.

El personal que opera la AR tiene las siguientes obligaciones:

1. Realizar sus operaciones de acuerdo con este documento.
2. Mantener las herramientas de tratamiento de certificados electrónicos bajo su estricto control.

3. Formalizar el contrato de certificación con la persona solicitante, según la política establecida.

4. Verificar fehaciente y exhaustivamente la identidad y cualquier otro dato personal de la persona que solicita los certificados, que sea relevante para el propósito de estos. Para ello se requerirá la presencia física de dicha persona, que deberá presentar DNI o NIE original y en vigor. Alternativamente se podrá permitir la identificación de la persona solicitante mediante la presentación de una solicitud firmada con un certificado electrónico reconocido, sin necesidad de personación física.

5. Informar a las personas solicitantes de certificados de las condiciones precisas de utilización de los mismos y de sus limitaciones de uso.

6. Transmitir de manera segura a las AC las solicitudes de certificados debidamente verificadas, con toda la información relevante que proporcionase la persona solicitante, así como las de revocación, suspensión o levantamiento de suspensiones de certificados.

7. Recibir los certificados emitidos de manera igualmente segura.

8. Almacenar de forma segura tanto la documentación aportada por la persona solicitante como la generada por la propia AR durante los procesos de registro o de revocación. Esta información se deberá conservar durante, al menos, quince años.

9. En caso de aprobación de una solicitud de certificación o renovación, notificar al suscriptor la emisión de su certificado.

10. En caso de rechazo de una solicitud de certificación, renovación, revocación, suspensión o levantamiento de suspensión, notificar al solicitante dicho rechazo y su motivación.

11. Mantener la confidencialidad de la información manejada durante y después de la prestación de los servicios.

AUTORIDAD DE VALIDACIÓN

La AV es el componente de la PKI responsable de proporcionar mecanismos que permitan que los usuarios de la PKI puedan comprobar en cada momento que siguen siendo válidos los certificados electrónicos empleados para firmar documentos electrónicos o para la identificación de entidades.

En la PKI-PA esta función se prestará a través del sistema de información que el personal técnico del Servicio de Informática despliegue a tal efecto, que proporcionará las siguientes funcionalidades:

1. Un servicio de validación de certificados mediante el protocolo OCSP, estándar técnico definido en el RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP), como mecanismo principal para la validación de los certificados. Este servicio solo se ofrecerá desde una URL de acceso exclusivamente interno a la institución.

Las respuesta de este servicio debe ir firmada electrónicamente y, para evitar riesgos derivados de mantener continuadamente en memoria la clave privada de la AC emisora, se firmarán con un certificado electrónico específico de OCSP. Para evitar bucles infinitos en el proceso de validación, este certificado no puede ser validado, por lo que debe tener un periodo de vigencia de seis meses, con objeto de minimizar el impacto de un posible compromiso del mismo.

2. Publicación de listas de revocación y suspensión de certificados (CRL) a través del protocolo HTTP empleando URL de acceso exclusivamente interno a la institución, como mecanismo de respaldo para la validación de los certificados ante la indisponibilidad del servicio OCSP.

USUARIOS

Los titulares de certificados electrónicos de la PKI-PA son aquellas personas físicas que cuentan con certificados electrónicos emitidos a su nombre por la PKI para la realización de firmas electrónicas. Estos usuarios tienen las siguientes obligaciones:

1. Proporcionar a la AR información exacta y completa en relación con los datos que se les soliciten durante el proceso de registro.

2. Custodiar los datos de creación de firma asociados a sus certificados que les pudiesen ser entregados, sin cederlos a ninguna otra persona o sistema, salvo autorización expresa para su uso en los sistemas de información del PA, conforme al procedimiento establecido al respecto en el presente documento.

3. Limitar y adaptar el uso del certificado a fines lícitos y de conformidad con los usos permitidos por la normativa existente y por este documento.

4. Solicitar inmediatamente la revocación de un certificado en caso de conocimiento o sospecha del compromiso de la clave privada asociada a su clave pública. Esta solicitud debe realizarla conforme al procedimiento establecido al efecto en este documento.

5. No utilizar certificados electrónicos cuyo periodo de validez haya expirado o hayan sido revocados o suspendidos.

6. Firmar el contrato de aceptación del certificado, lo que implica conocer y aceptar la política de certificación del PA.

7. Destruir las claves privadas que pudiesen custodiar de certificados que les hayan sido revocados. Si estas se almacenasen en dispositivos criptográficos seguros del Parlamento, deberá devolverlos inmediatamente al Parlamento, para su destrucción segura.

8. Asumir la responsabilidad por los daños y perjuicios que se causen a sí mismos o a terceros si incurren en alguno de los siguientes supuestos:

   1.1. Negligencia en la conservación de los datos de creación de firma.

   1.2. No solicitar la suspensión del certificado, en caso de duda sobre el mantenimiento de la confidencialidad de los datos de creación de firma.

   1.3. No solicitar la revocación del certificado, en caso de certeza sobre el mantenimiento de la confidencialidad de los datos de creación de firma.

   1.4. Utilizar los datos de creación de firma si el certificado ha sido revocado o suspendido.

   1.5. No utilizar el certificado de acuerdo con las condiciones establecidas por la AC del PA.

Las partes confiables son los usuarios de la PKI-PA que trabajan con documentos firmados electrónicamente por titulares de esta. Tienen las siguientes obligaciones:

1. Verificar la validez de las firmas electrónicas de los documentos con los que trabajan, conforme a las herramientas que les ofrezcan para ello las aplicaciones a través de las que los manipulen, asumiendo las responsabilidades derivadas de su incorrecta comprobación.

2. Confiar en las firmas electrónicas basadas en certificados electrónicos emitidos por las AC del PA que superen las pruebas de validez realizadas por las herramientas a través de las que se manipulen, siempre que se utilicen dentro de su ámbito de aplicación y conforme a las posibles extensiones sobre capacidades y restricciones de uso que pudiesen incorporar.

El personal que opere los sistemas de la PKI tiene las siguientes obligaciones:

1. Mantener la confidencialidad de la información manejada durante y después de la prestación de los servicios y custodiarla con la debida diligencia.
2. Asistir a la formación en seguridad y procedimientos de PKI que le imparta el PA.
3. Comunicar cualquier incidente de seguridad detectado a través de los canales establecidos al efecto.

PROCEDIMIENTOS

GENERACIÓN DE CLAVES Y CERTIFICADOS DE AC

Las claves de las AC se generarán desde el mismo equipo sobre el que estas vayan a operar, para evitar los riesgos derivados de su traslado, y se almacenarán en un contenedor que no permita la exportación de la clave privada. Este equipo se mantendrá debidamente securizado conforme a la línea base de seguridad establecida en la normativa de seguridad del PA. A él solo tendrá acceso el personal técnico que el Servicio de Informática haya específicamente formado y autorizado al efecto, que empleará cuentas nominativas, con identificación basada en un certificado electrónico reconocido.

El certificado de la AC raíz incluirá los siguientes atributos y extensiones:

Subject que indique que el titular del certificado es la AC raíz del PA, siguiendo el siguiente formato, que, conforme al estándar X.509, lo expresa como DN, con atributos del estándar X.501:

C=ES, O=Parlamento de Andalucía, OU= Servicio de Informática, CN=AC Raíz Parlamento de Andalucía

Donde:

- *C (Country)*: país al que pertenece el titular del certificado: ES = España.
- *O (Organization)*: organización a la que pertenece el titular del certificado: Parlamento de Andalucía.
- *OU (Organizational Unit)*: unidad organizativa a la que está adscrito el titular del certificado: el Servicio de Informática del PA, que es quien gestiona la AC raíz.
- *CN (Common Name)*: titular de certificado: AC Raíz Parlamento de Andalucía.

- *BasicContraints* con valor CA=TRUE, para indicar que el certificado corresponde a una AC.
- *KeyUsage* con valor keyCertSign, cRLSign, para indicar que el certificado puede usarse para firmar certificados y CRL.
- *CDP* con la URL de la CRL de la AC emisora del certificado, que es ella misma.
- *CertificatePolicies* con identificador y URL interna de esta CPS.
- *SKI* con la huella digital de la clave pública del certificado, empleada para facilitar su localización en el almacén de certificados del cliente cuando se vaya a validar una firma.

Los certificados de las AC intermedias incluirán los siguientes atributos y extensiones:

- *Subject* que indique que la AC intermedia a la que pertenece el certificado siguiendo un formato DN equivalente al de la AC raíz en el que se cambie el nombre del titular por AC, seguido

del nombre del grupo parlamentario al que corresponde la AC o «diputados no adscritos», para la AC correspondiente a los disputados no adscritos. Ejemplos:

C=ES, O=Parlamento de Andalucía, OU= Servicio de Informática, CN=AC Grupo Popular

C=ES, O=Parlamento de Andalucía, OU= Servicio de Informática, CN=AC Diputados No adscritos

- *BasicContraints* con valor CA=TRUE, para indicar que el certificado corresponde a una AC.
- *KeyUsage* con valores keyCertSign, cRLSign, para indicar que el certificado puede usarse para firmar certificados y CRL.
- *AIA*[14], con las URL del certificado de la AC raíz y del servicio OCSP de la AV, que serán internas, solo accesibles desde la LAN de la institución.
- *CDP* con las URL de la CRL de la AC raíz, que es quien emitió el certificado.
- *CertificatePolicies*: identificador, URL interna y descripción de la CPS de la PKI-PA.
- *SKI*: Huella digital de la clave pública del certificado, para facilitar su localización entre los demás certificados incluidos en la firma o, en su defecto, en el almacén de certificados del cliente cuando se vaya a validar una firma.
- *AKI*: Huella digital de la clave pública de la AC raíz que emitió el certificado, para facilitar su localización en el almacén de certificados del cliente, cuando se vaya a validar una firma.

GENERACIÓN DE CERTIFICADOS DE USUARIO PARA FIRMA AUTOMATIZADA

Los usuarios solicitarán la generación inicial y la renovación de los certificados a través de la plataforma de soporte al usuario del Servicio de Informática, desde donde se les concertará cita presencial o por videoconferencia para su emisión y se les indicará la documentación identificativa que deben aportar. Una vez validada esta documentación, se les generará el certificado y se instalará en la aplicación para la firma de iniciativas. El certificado estará protegido por una contraseña que se les transmitirá de manera privada a través de correo electrónico seguro. Se conservará evidencia documental de todo el proceso.

Los certificados de usuario incluirán los siguientes atributos y extensiones:

- *Subject* que indique el nombre completo del titular del certificado y su DNI o NIE en forma de DN, tal y como se muestra en el siguiente ejemplo (ficticio):

C=ES, O=Parlamento de Andalucía, serialNumber=IDESP-12345678Z, CN=Juan Pérez García

Donde se emplean los siguientes atributos X.501:

- *C*: con valor ES, para indicar que la persona titular del certificado es española.
- *O*: con valor Parlamento de Andalucía, para indicar que el titular trabaja para el PA.
- *serialNumber*: con el DNI o NIE de la persona titular como valor conforme al formato requerido por la norma ETSI EN 319 412, empleada para certificados cualificados en la UE. Este formato requiere incluir un prefijo IDESP- para denotar que es un documento oficial de identificación emitido por el Estado español.
- *CN*: con el nombre completo de la persona titular como valor tal cual aparece en el documento de identificación presentado por esta. No se admiten seudónimos.

[14] Authority Information Access

• *BasicContraints* con valor CA=FALSE, para indicar que la persona titular no es una AC.

• *KeyUsage* con valor digitalSignature, para indicar que el certificado solo puede usarse para realizar firmas electrónicas.

• *ExtendedKeyUsage* con valor contentCommitment, para indicar que las firmas realizadas con el certificado expresan la aceptación, aprobación y compromiso del firmante con el contenido firmado.

• *AIA*, con las URL del certificado de la AC intermedia que emitió el certificado y del servicio OCSP de la AV, que serán internas, solo accesibles desde la LAN de la institución

• *CDP* con las URL de la CRL completa de la AC emisora del certificado y de su delta, que serán internas, solo accesibles desde la LAN de la institución

• *CertificatePolicies*: identificador, URL interna y descripción de la CPS de la PKI-PA.

• *AKI*: Huella digital de la clave pública de la AC intermedia que emitió el certificado, para facilitar su localización entre los demás certificados incluido en la firma o, en su defecto, en el almacén de certificados del cliente cuando se vaya a validar una firma.

RENOVACIÓN DE CERTIFICADOS

La AC del PA que genera cada certificado enviará a su titular un email de aviso de caducidad un mes antes del fin del periodo de validez de este.

Las solicitudes de renovación de certificados cuyo periodo de validez no haya caducado se podrán presentar desde un mes antes de su caducidad a través de la plataforma de soporte al usuario del Servicio de Informática. Bastará firmar la solicitud con el certificado vigente, sin necesidad de personación.

La renovación de certificados cuyo periodo de validez vaya a caducar se realizará siguiendo el mismo procedimiento que la generación inicial del certificado.

REVOCACIÓN DE CERTIFICADOS

La revocación de los certificados consiste en la inhabilitación permanente de los mismos a partir de una cierta fecha. Podrá producirse por los siguientes motivos:

Tener constancia de que se ha visto comprometida la seguridad de su clave privada por robo, pérdida, divulgación, debilidad criptográfica o cualquier otro motivo.

Contener información inexacta. Por ejemplo, si el usuario cambia de nombre o si deja de pertenecer al grupo parlamentario cuya AC emitió el certificado.

Jubilación, cese o fallecimiento del titular.

Detectar uso indebido del certificado o de sus claves asociadas, incumpliendo los requisitos operativos de su contrato o de este documento.

Compromiso de la clave privada de la AC que emitió el certificado o de alguna AC superior.

Solicitud del titular del certificado, orden judicial o solicitud de tercero que tenga expresa autorización escrita previa del titular.

Le revocación podrá realizarse de varias formas:

• *A iniciativa del titular o de tercero autorizado*: este deberá solicitar la revocación a través de la plataforma de soporte al usuario del Parlamento, donde se tratará con prioridad urgente.

• *A iniciativa del PA u orden judicial*: cuando el PA tenga constancia de que se ha producido alguna de las circunstancias ante las que cabe revocación de un certificado emitido por sus AC o reciba orden judicial al respecto, efectuará su revocación inmediata.

Cada vez que un certificado sea revocado, el PA debe avisar al usuario por correo electrónico e iniciar automáticamente el proceso de concertación de cita para la emisión de uno nuevo a través de la plataforma de soporte al usuario del Parlamento, salvo que el usuario haya manifestado su deseo de lo contrario o por la naturaleza de la revocación esto sea improcedente.

SUSPENSIÓN DE CERTIFICADOS

La suspensión de certificados consiste en la inhabilitación temporal de los mismos a partir de una cierta fecha ante:

• Sospecha de haber concurrido alguna circunstancia que podría requerir de su revocación. Se procederá a la inmediata revocación del certificado en cuanto se confirme dicha sospecha y se rehabilitará el certificado si se confirma que la sospecha era infundada.

• Recepción de revocación sin verificación posible de la identidad del solicitante.

Si tras un máximo de 30 días naturales no se dan las circunstancias necesarias para rehabilitar un certificado suspendido, este se revocará automáticamente para proteger la seguridad del titular.

PUBLICACIÓN DE CRL

La ubicación de las listas de certificados revocados y suspendidos por cada AC se publicará a través del atributo CDP incluido en los certificados emitidos por esta, que contendrán direcciones URL internas (no accesibles desde fuera de la institución) que apunten mediante HTTPS a dos tipos de listas firmadas electrónicamente por la AC:

• *CRL completa*, con los números de serie de todos los certificados emitidos por la AC que hayan sido revocados desde que se creó la clave privada de esta, así como los de los certificados que se encuentren suspendidos.

• *CRL delta*, con los números de serie de todos los certificados emitidos por la AC que hayan sido revocados, suspendidos o reactivados desde la última CRL completa publicada.

AUTORIZACIÓN DE FIRMA

Los titulares de los certificados electrónicos podrán conceder y revocar la autorización de solicitud de firmas en su nombre a otros titulares de certificados electrónicos a través de la herramienta que a tal efecto les proporcione el Parlamento. Estas operaciones se registrarán con trazabilidad completa.

REEMISIÓN POR CAMBIO DE GRUPO PARLAMENTARIO

Cuando el PA tenga constancia de que ha cambiado la pertenencia a un grupo parlamentario del titular de un certificado electrónico emitido por su PKI, lo revocará inmediatamente. La AC intermedia correspondiente a su nuevo grupo le emitirá un nuevo certificado que refleje su situación actual y se lo enviará a su correo electrónico corporativo de manera segura. Asimismo, el Parlamento cargará este nuevo certificado en las aplicaciones que tuviesen cargado el antiguo, sustituyéndolo y dando de baja todas las autorizaciones de firma en su nombre que pudiese tener habilitadas.

TERMINACIÓN DE LA AC

Cuando la seguridad de los datos de creación de firma de una AC se vea comprometida o se decida el cese de la actividad de esta, el Servicio de Informática ejecutará las siguientes acciones de terminación de la AC:

1. *Revocar todos los certificados* emitidos por la AC, avisando por correo electrónico a todos los titulares de certificados. Si la terminación es por cese de la AC, los avisos se emitirán con, al menos, un mes de antelación a la fecha planificada de cese. Si la terminación es por compromiso de datos de creación de firma, el aviso se realizará justo a continuación de la inmediata revocación de los certificados.
2. *Publicar una CRL final completa* con todas las revocaciones efectuadas, que se mantendrá hasta que finalice el periodo de validez de todos los certificados emitidos, más un periodo de retención adicional de seis meses.
3. *Borrar los datos de creación de firma* de la AC mediante un procedimiento seguro de purga conforme a la guía NIST 800-88.
4. *Mantener durante quince años el repositorio* de la AC, salvo archivos temporales y datos de creación de firma.

GESTIÓN DE INCIDENTES

Todo incidente que afecte a la seguridad de la infraestructura PKI (compromisos de claves privadas, accesos no autorizados a sistemas, emisión incorrecta o fraudulenta de certificados, caídas de servicio, pérdida de registros o de auditorías, errores de configuración con impacto en la seguridad, etc.) y sea detectado por sistemas de monitorización o por personas físicas se gestionará conforme al siguiente procedimiento:

1. *Notificación*: el incidente se notificará inmediatamente al Servicio de Informática a través de la dirección de correo electrónico seguridad@parlamentodeandalucia.es. Si el incidente afecta a titulares de certificados electrónicos emitidos por la PKI-PA, el Servicio de Informática lo notificará a los afectados en menos de 24 horas, también por correo electrónico.
2. *Análisis y clasificación*: el CSIRT-PA recopilará todas las evidencias que sean pertinentes según la naturaleza del incidente (logs de aplicaciones y del sistema operativo, testigos, etc.) y evaluará el impacto del mismo sobre las claves privadas, certificados emitidos, integridad del

repositorio de la PKI y disponibilidad de los servicios. En base a ello clasificará el incidente como crítico, mayor o menor.

3. *Contención*: según la clasificación y tipo del incidente, el CSIRT-PA aplicará las medidas necesarias para limitar su impacto y la propagación. Esto puede incluir, entre otras acciones, bloquear accesos involucrados, aislar sistemas implicados, deshabilitar servicios afectados y revocar certificados comprometidos.

4. *Erradicación*: una vez contenido el incidente, el CSIRT-PA aplicará las medidas necesarias para eliminar la amenaza o causa raíz del incidente. Esto puede incluir, entre otras acciones, corregir configuraciones, cambiar credenciales de acceso, aplicar parches de seguridad, desinstalar los software vulnerables, eliminar malware, reinicializar sistemas y restaurar desde respaldos verificados.

5. *Recuperación*: una vez erradicado el incidente, el CSIRT-PA aplicará las medidas que sean necesarias para restaurar el funcionamiento normal de la PKI y asegurar que todo funciona correctamente, sin riesgo de repetición del incidente. Esto puede incluir, entre otras acciones, reemitir certificados y aplicar temporalmente una monitorización específica y reforzada del funcionamiento de los sistemas.

6. *Documentación y registro*: una vez recuperado el sistema, el CSIRT-PA registrará información detallada sobre el incidente que incluya código de identificación, título, descripción detallada, impacto, fechas y horas de detección, contención, erradicación y recuperación, quién lo detectó, impacto, acciones tomadas, evidencias conservadas y lecciones aprendidas. Esta documentación se debe conservar durante quince años, al menos.

7. *Mejora continua*: tras el cierre del incidente se realizará un análisis post mortem, para revisar controles internos, evaluar fallos en el proceso, implementar mejoras técnicas o procedimentales y, si procede, actualizar esta declaración de prácticas de conformidad.

Este procedimiento de gestión de incidentes será revisado anualmente por el Servicio de Informática.

MEDIDAS DE SEGURIDAD

Para garantizar la seguridad del funcionamiento de la PKI-PA se establecen las siguientes medidas de seguridad:

1. *Bastionado*: los equipos sobre los que se implementen los principales componentes de la PKI ejecutarán sistemas operativos endurecidos, con control estricto de accesos y registros centralizados en SIEM.

2. *Acceso interno*: el servicio OCSP y las CRL que permitan validar los certificados solo se ofrecerán a través de direccionamiento IP privado, no siendo accesibles desde fuera de la institución.

3. *Copias de seguridad*: periódicamente se realizarán copias de seguridad cifradas y distribuidas en varias ubicaciones de todos los sistemas sobre los que se apoye la PKI, para garantizar la continuidad de negocio en caso de incidentes.

4. *Borrado seguro*: se aplicarán técnicas de borrado seguro para la limpieza de todos los equipos y soportes donde temporalmente se almacenen datos de creación de firma que garanticen que no sea posible recuperar dichos datos.

5. *Registro de eventos*: se registrarán los eventos relacionados con el funcionamiento de la PKI-PA más significativos desde el punto de vista de la seguridad, lo que incluye:

- Intentos exitosos y fallidos de administración de certificados: inicio y cierre de sesiones en las aplicaciones y sistemas operativos sobre los que se implemente la PKI, gestión de cuentas de usuario, emisión y revocación de certificados, archivado y recuperación de claves, accesos al repositorio de certificados emitidos, etc.
- Publicación de CRL.
- Cambios en la configuración de los componentes de la PKI.
- Copias de seguridad y restauraciones de la base de datos de las AC.
- Inicio y apagado de las aplicaciones y sistemas operativos en que se apoye la PKI.
- Cambios en la política de la PKI.

6. *Monitorización*: el SOC-PA realizará una monitorización continua de estos eventos y del funcionamiento de la PKI-PA, y el CSIRT-PA responderá a las amenazas detectadas.

7. *Auditoría*: el SOC-PA realizará una auditoría de seguridad anual de la PKI-PA y auditorías extraordinarias ante cambios significativos en la misma, proporcionando un plan de acción correctivo para las no conformidades y apoyo en la aplicación del mismo.

8. *Revisiones*: revisión anual de la DCP y, en especial, de la adecuación de su perfil técnico al estado del arte.

PERFIL TÉCNICO

La siguiente tabla recoge los principales parámetros técnicos por los que se rige el funcionamiento de la PKI-PA, los cuales se revisarán anualmente para mantenerlos adaptados al estado del arte:

Parámetro	Valor
Algoritmo de claves	ECDSA P-384 en certificados de AC ECDSA P-256 en certificados de usuario y de respuestas OCSP
Algoritmo de firma electrónica	SHA384withECDSA en certificados de usuario y de respuestas OCSP SHA256withECDSA en certificados de usuario y de respuestas OCSP
Validez de certificados	AC Raíz: 25 años AC intermedia: 10 años Certificado de usuario: 4 años Certificado de respuesta OCSP: 6 meses
Validez de respuestas OCSP	4 horas
Periodicidad de actualización de CRL	24 horas
Avisos de caducidad de certificados	1 mes antes de fin de validez
Máxima duración de suspensión de certificados	30 días naturales, tras los que se revocan
Retención de datos	15 años

Parámetro	Valor
Atributos y extensiones de certificado de AC raíz	+ BasicContraints: *CA=True, CRITICAL, pathLenConstraint=1* + KeyUsage: *keyCertSign, cRLSign, CRITICAL* + CDP: http://crl.parlamento-and.es/ac-raiz + Subject: *C=ES, O=Parlamento de Andalucía, OU= Servicio de Informática, CN=AC Raíz Parlamento de Andalucía* + SKI: [Huella digital de clave pública de AC raíz] + AKI: [Huella digital de clave pública de AC raíz] + Certificate Policies: - Policy: 1.3.6.1.4.1.193147254.0.1 (pendiente de solicitud) - CPS: https://intranet.parlamento-and.es/PKI/CPS.pdf
Atributos y extensiones de certificados de AC intermedia	+ BasicContraints: *CA=True,CRITICAL pathLenConstraint=0* + KeyUsage: *keyCertSign, cRLSign, CRITICAL* + CDP: http://crl.parlamento-and.es/ac-raiz + AIA: - Emisor: http://intranet.parlamento-and.es/PKI/ac-raiz.crt - Validación OCSP: http://ocsp.parlamento-and.es + Subject: *C=ES, O=Parlamento de Andalucía, OU= Servicio de Informática, CN=AC* [Grupo X o Diputados no adscritos] + SKI: [Huella digital de clave pública de AC intermedia] + AKI: [Huella digital de clave pública de AC raíz] + Certificate Policies: - Policy: 1.3.6.1.4.1.193147254.1.[número específico de la AC intermedia emisora] - CPS: https://intranet.parlamento-and.es/PKI/CPS.pdf
Atributos y extensiones de certificados de usuario para firma automatizada	+ BasicContraints: *CA=False* + KeyUsage: *digitalSignature, non-repudiation* (contentCommitment), *CRITICAL* + CDP: http://crl.parlamento-and.es/ac-grupo-X + AIA: - Emisor: http://intranet.parlamento-and.es/PKI/ac-grupo-X.crt - Validación OCSP: http://ocsp.parlamento-and.es + Subject: *C=ES, O=Parlamento de Andalucía, serialNumber=IDESP-*[DNI/NIE], *CN=*[nombre completo] + AKI: [Huella digital de clave pública de AC intermedia que emitió el certificado] + Certificate Policies: - Policy: 1.3.6.1.4.1.193147254.2.1 - CPS: https://intranet.parlamento-and.es/PKI/CPS.pdf

Parámetro	Valor
Atributos y extensiones de certificados de respuestas OCSP	+ BasicContraints: *CA=False* + KeyUsage: *digitalSignature, CRITICAL* + ExtendedKeyUsage*: id-kp-OCSPSigning, contentCommitment* + id-pkix-ocsp-nocheck: presente + CDP: http://crl.parlamento-and.es/ac-grupo-X + AIA: - Emisor: http://intranet.parlamento-and.es/PKI/ac-grupo-X.crt - Validación OCSP: http://ocsp.parlamento-and.es + Subject: *C=ES, O=Parlamento de Andalucía, CN=OCSP AC* [Nombre de AC emisora] + AKI: [Huella digital de clave pública de AC intermedia que emitió el certificado] + Certificate Policies: - Policy: 1.3.6.1.4.1.193147254.2.2 - CPS: https://intranet.parlamento-and.es/PKI/CPS.pdf

PUBLICIDAD

En el portal institucional se publicarán las prácticas de certificación de la PKI-PA, los certificados de sus AC, sus huellas digitales y el estado de validez de estos. Toda esta documentación se publicará firmada electrónicamente para garantizar su autenticidad e integridad.

Adicionalmente, se proporcionarán los siguientes canales de contacto para solicitar más información y aclarar dudas sobre las prácticas de certificación de la PKI-PA:

- *Email*: pki@parlamentodeandalucia.es
- *Teléfono*: 954 59 21 00
- *Dirección*: C\ San Juan de Ribera, s/n. 41009 Sevilla

La información de la PKI-PA publicada tendrá carácter de privada, solo autorizándose el acceso a ella al personal que tenga concedido permiso de conexión a la red interna de la institución.

Tiene consideración de confidencial la siguiente información manejada por la PKI-PA, no permitiéndose su divulgación a terceros, salvo autorización expresa, previa y por escrito del letrado mayor del Parlamento de Andalucía, caso en que la obligación de confidencialidad se transferirá a dichos terceros.

La información transferida incluirá:

1. Claves privadas.
2. Datos de carácter personal proporcionados para la obtención de los certificados.
3. Detalles de la operativa interna, incluidos parámetros de seguridad y control, así como procedimientos de auditoría.

REVISIÓN Y APROBACIÓN

Este documento será revisado anualmente por el Comité de Seguridad de la Información.

Su aprobación corresponde a la Mesa del Parlamento de Andalucía.