DOCUMENTO DE ACEPTACIÓN DE LOS CERTIFICADOS DE INDENTIDAD PÚBLICA CONTENIDOS EN EL DOCUMENTO NACIONAL DE IDENTIDAD ELECTRONICO

La obtención del documento nacional de identidad electrónico presupone la aceptación de los Certificados de autenticación y firma emitidos por la Autoridad de Certificación del DNI electrónico, (Dirección General de la Policía (DGP) –Ministerio del Interior -), así como las condiciones establecidas para su titularidad y uso posterior.

Dichas condiciones están recogidas en el documento de Declaración de Prácticas y Políticas de Certificación, accesible en la dirección www.dnielectronico.es

---

Este documento constituye una síntesis del contenido, derechos y obligaciones establecidos en la Declaración de Prácticas y Políticas de Certificación (DPC) y tiene como objetivo informar del deber de la Dirección General de la Policía como Prestador de Servicios de certificación de proporcionar al solicitante antes de la expedición de los certificados la información mínima recogida en el artículo 18 b) de la Ley 59/2003 de firma electrónica.

Es obligada la lectura completa de la DPC para entender los objetivos, especificaciones, normas, derechos, obligaciones y responsabilidades que rigen la prestación del servicio de certificación.

Objeto. Aspectos Generales

- ✓ La **Ley 59/2003**, de **19 de diciembre**, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.
- ✓ El registro de certificación de los ciudadanos españoles se realizará en los lugares de expedición del DNI en el mismo momento en que se proceda a dicha expedición, tal y como regula el **Real Decreto 1553/2005, de 23 de diciembre**.

DPC

- ✓ La DPC y los documentos relacionados regulan todo el ciclo de vida de los certificados electrónicos desde su solicitud hasta su extinción o revocación, así como las relaciones que se establecen entre el solicitante/titular del certificado, la Autoridad de Certificación y los terceros aceptantes.
- ✓ Se establece la delimitación de responsabilidades de las diferentes partes intervinientes así como las limitaciones de las mismas ante posibles daños y perjuicios.

Características de los Certificados. Condiciones de Uso

- ✓ Los Certificados de Identidad Pública serán emitidos como **Certificados Electrónicos Reconocidos** cumpliendo los requisitos del anexo I de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma

electrónica, así como lo dispuesto a tal efecto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- ✓ Los certificados emitidos tendrán un periodo máximo de validez de treinta meses desde el día en qué sean emitidos, figurando en los mismos la fecha de caducidad.
- ✓ Los Certificados de Identidad Pública, emitidos por la Dirección General de la Policía (Ministerio del Interior) tendrán como finalidad:
    - o **Certificado de Autenticación:** Garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática.
    - o **Certificado de Firma**: El propósito de este certificado es permitir al ciudadano firmar electrónicamente trámites o documentos, y de acuerdo a la LFE 59/2003 tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- ✓ El perfil de los certificados no contempla el uso de dichos certificados y sus claves asociadas para cifrar ningún tipo de información.
- ✓ La generación de claves se realizará en la tarjeta y en presencia del titular, tras la habilitación de una clave personal de acceso –PIN- aleatoria que se entrega al ciudadano en forma de sobre ciego. Dicha clave de acceso es confidencial, personal e intransferible y es el parámetro que protege sus claves privadas. La clave de acceso – PIN - podrá ser cambiada de forma confidencial por otra de la elección del ciudadano.
- ✓ Tal y como recoge el Real Decreto ***1553/2005*** la activación del dispositivo de creación de firma tendrá carácter voluntario, por lo que el ciudadano podrá solicitar la revocación de los certificados emitidos como parte del proceso de expedición.
- ✓ Si el usuario no manifiesta la intención de revocar dichos certificados tras la expedición, se dará por confirmada la aceptación de los mismos, así como de sus condiciones de uso.
- ✓ En la Infraestructura de Clave Pública adoptada para el DNI electrónico, se ha asignado a entidades/organismos diferentes de la DGP las funciones de **Autoridad de Validación**. Para la validación del DNIe se dispone de varios prestadores de Servicios de Validación que proporcionan información sobre el estado de los certificados emitidos por la jerarquía de certificación del DNIe.

Obligaciones y responsabilidades del subscriptor

Se entiende por subscriptor del certificado al ciudadano español, con plena capacidad de obrar, que voluntariamente confía y hace uso de los certificados contenidos en su Documento Nacional de Identidad y emitidos por la Dirección General de la Policía (Ministerio del Interior), de los cuales es titular.

Es obligación de los titulares de los certificados:

- ✓ Suministrar a las Autoridades de Registro información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.
- ✓ Conocer y aceptar las condiciones de utilización de los certificados.
- ✓ Conservar y utilizar de forma correcta el Documento Nacional de Identidad y los Certificados y claves.

- ✓ Comunicar a la Dirección General de la Policía, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento de la tarjeta.
- ✓ Proteger sus claves privadas y custodiar los Cerificados asociados, tomando las precauciones razonables para evitar su pérdida, revelación, alteración o uso no autorizado.
- ✓ Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada, entre otras causas por: pérdida o sustracción. La forma en que puede realizarse esta solicitud se encuentra especificada en www.dnielectronico.es
- ✓ Cumplir las obligaciones que se establecen para el suscriptor en la DPC y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- ✓ El ciudadano asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.
- ✓ Así mismo el ciudadano se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al ciudadano.

Obligaciones y responsabilidades de la Dirección General de la Policia

La DGP como prestador de servicios de certificación en la expedición del DNIe:

- ✓ Actuará relacionando una determinada clave pública con su titular a través de la emisión de los certificados, de conformidad con los términos de la DPC.
- ✓ Los servicios prestados por la DGP en el contexto de la DPC son los servicios de emisión, renovación y revocación de los certificados.
- ✓ La DGP comunicará los cambios de la DPC de acuerdo con lo establecido en el propio documento.
- ✓ Emitirá certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- ✓ Revocará los certificados en los términos recogidos en la DPC y pondrá a disposición de los titulares y terceros aceptantes de los certificados, la información de estado de los certificados a través de los prestadores de servicios de validación.
- ✓ Pondrá a disposición de los ciudadanos los certificados correspondientes a la(s) Autoridad(es) de Certificación de la Dirección General de la Policía (Ministerio del Interior).
- ✓ Protegerá la clave privada de la(s) Autoridad(es) de Certificación de la Dirección General de la Policía (Ministerio del Interior).
- ✓ Utilizará sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte
- ✓ No almacenará en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados de identidad pública.
- ✓ La Dirección General de la Policía (Ministerio del Interior) responderá por los daños y perjuicios que causen a cualquier ciudadano en el ejercicio de su

actividad cuando incumpla las obligaciones que les impone la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- ✓ La Dirección General de la Policía (Ministerio del Interior) no será responsable del contenido de aquellos documentos firmados electrónicamente por los ciudadanos con el Certificado de Identidad Pública contenido en el DNI.

Garantías

- ✓ A excepción de lo establecido por las disposiciones de la DPC, la DGP no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

Protección de Datos de Carácter personal

- ✓ El titular de los certificados conoce que los datos facilitados serán cargados en ficheros automatizados titularidad de la DGP con la finalidad de la gestión de la PKI y la generación de los certificados digitales. Asimismo, conoce la forma de ejercer sus derechos de acceso, rectificación, cancelación y oposición.
- ✓ Los datos contenidos en el Directorio seguro de Certificados tienen la consideración de datos de carácter personal a efectos de lo dispuesto en la LOPD y demás normativa complementaria, y por este motivo, no se permite el acceso por terceros. No obstante, se pone a disposición de los prestadores de servicios de validación las listas de certificados revocados, que no contienen datos personales, para el cumplimiento diligente de los servicios de certificación. El usuario de estas listas únicamente podrá utilizar su contenido de acuerdo con esas finalidades

Legislación aplicable y jurisdicción competente

- ✓ Se considera normativa básica aplicable:
  - *Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.*
  - *Ley 59/2003, de 19 de diciembre, de Firma Electrónica.*
  - *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.*
  - *REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica*
- ✓ La jurisdicción competente será la Contencioso Administrativa.

Para más información, consulte la página web establecida al efecto cuya dirección es http://www.dnielectronico.es o póngase en contacto con la Autoridad de Certificación mediante la dirección de correo electrónico certificados@dnielectronico.es.

Servicio Atención al Ciudadano sac@dnielectronico.es Teléfono 900 364 463