
Contrato Certificado digital

° Anverso: ° Reverso: ° Tipo de documento:
° Documento de identidad:
° Nombre:
° Primer apellido: ° Segundo apellido:
° Fecha de Nacimiento: ° Fecha de validez: ° Nacionalidad: ° Tipo documento:
° Genero: ° Número de soporte físico: ° Correo Electrónico:
° Confirmación de correo electrónico: ° Apellidos:

Se informa al solicitante que durante el proceso de validación de sus datos para proceder a emitir el certificado digital se realizarán mecanismos de identificación remota por vídeo, los cuales seguirán las recomendaciones de seguridad aplicables, así como de lo previsto en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016. Si continua con el proceso usted nos autoriza y consiente de forma expresa que acepta que se realice la grabación íntegra del vídeo y al tratamiento y conservación de categorías especiales de datos personales.

Por la presente autorizo de forma expresa a la grabación íntegra del vídeo y al tratamiento y conservación de categorías especiales de datos personales, con el fin de realizar el proceso de identificación remota. Si no desea realizar este proceso deberá personarse físicamente en nuestras oficinas para concluir el proceso.

Datos de dirección del suscriptor

° Dirección: ° País: ° Provincia: ° Población:
° Provincia Texto: ° Población Texto: ° codigopais:
° Descripción: **Certificado digital - Emitido por inDenova SUB CA 003**

Solicito la expedición del Certificado digital y declaro conocer y aceptar las condiciones de utilización, así como lo dispuesto en la Declaración General de Prácticas de Certificación y en las Políticas y Prácticas de Certificación.

El Solicitante manifiesta que es mayor de edad o menor emancipado y que está en posesión de un documento para su identificación (DNI - NIF - NIE), que los datos aquí mostrados son veraces, asumiendo cualquier responsabilidad sobre la realidad de las declaraciones vertidas y sobre el uso del Certificado.

El Solicitante manifiesta que, una vez descargue e instale el Certificado en su equipo, adquirirá la condición de Titular (suscriptor) y utilizará el Certificado de conformidad con las condiciones adjuntas y atendiendo al contenido de la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y los de las Políticas y Prácticas Particulares Certificados Digitales existentes en <https://www.indenova.com/acreditaciones/eidas/>, declarando expresamente que las acepta en toda su extensión y que su capacidad no se encuentra limitada para contratar con esta Entidad.

Estos certificados electrónicos son cualificados en cumplimiento con los requisitos del Reglamento (UE) N° 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y por la que se deroga la directiva 1999/93/CE.

Las funcionalidades y propósitos de los Certificados Digitales permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones en las que participen sus Titulares.

TERMINOS DE USO Y ACEPTACIÓN DEL CERTIFICADO DIGITAL Por el presente documento, el titular del certificado digital manifiesta haber recibido un (01) certificado digital (uno de firma digital y autenticación asociado a su smartphone mediante el APP eSignalD, en un token o tarjeta criptográfica o en un enlace para su descarga e instalación en su equipo) y que él mismo ha activado, mediante su huella dactilar y/o con un código PIN, según corresponda.

Asimismo, manifiesta haber definido su PIN de acceso para el uso de sus certificados digitales, el cual es de su conocimiento exclusivo.

El titular se constituye en suscriptor de los certificados digitales emitidos por la ER Lleidanet PKI S.L. y es el único tenedor de los mismos. Por otro lado, manifiesta el titular del certificado digital que es conocedor que durante el proceso de emisión de los certificados digitales ha sido dado de alta en la plataforma www.esignabox.com propiedad de Lleidanet PKI S.L. y que acepta las condiciones de uso Versión 2.0 indicadas en la URL: https://www.esignabox.com/Documents/es/TermsOf Use_eSignaBox.pdf. La plataforma eSignaBox, será utilizada para enviarle documentos o transacciones de autenticación y firma digital, tanto de transacciones realizadas por la Entidad de Registro de Lleidanet PKI, la Entidad de Certificación de Lleidanet PKI, los colaboradores y puntos de verificación de Lleidanet PKI SL, la propia plataforma eSignaBox y terceras empresas que integren los servicios eSigna de Lleidanet PKI S.L. o sus filiales.

La aceptación de los certificados digitales supone que el titular reconoce estar de acuerdo y acepta los términos y condiciones contenidos en el presente documento así como las condiciones de la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y los de las Políticas y Prácticas Particulares Certificados Digitales existentes en <https://www.indenova.com/acreditaciones/eidas/>, el cual rige sus derechos y obligaciones, así como de la Entidad de Registro y de la Entidad de Certificación de Lleidanet PKI SL.

Con relación al uso de la clave privada y del certificado digital por parte del titular, este deberá de cumplir con lo siguiente:

1. Conocer y cumplir las condiciones de utilización de los certificados previstas en las condiciones de uso y en la Declaración de Prácticas de Certificación y en particular, las limitaciones de uso de los certificados.
2. Ser diligente en la custodia de sus claves y conservación de los datos de creación de firma o cualquier otra información sensible como claves, códigos de solicitud del certificado, contraseñas, etc. así como de los soportes de los certificados, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
3. Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.
4. Notificar a la Entidad de Registro sin retrasos injustificables: La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, smartphone, token criptográfico o tarjeta inteligente). El compromiso potencial de su clave privada o de su contraseña. La pérdida de control sobre su clave privada, debido al compromiso de su contraseña (datos de activación) o por cualquier otra causa. Las inexactitudes o cambios en el contenido del certificado digital.

Con relación a sus datos personales, el titular manifiesta haber sido informado de lo siguiente:

1. Que la Entidad de Registro o sus puntos de Verificación recogen únicamente datos personales o información de relevancia para la emisión de los certificados digitales.
2. Que los datos personales facilitados serán usados por Lleidanet PKI SL para el cumplimiento de los fines propios del Servicio de Certificación Digital y los correspondientes servicios de firma digital que pudieran utilizar dichos certificados.

3. Que el acceso a los datos personales estará únicamente limitada al titular y suscriptor del certificado digital y, de ser el caso, a los terceros que confían.
4. Que los datos personales podrán ser comunicados a otros organismos del Estado, dentro del marco de la colaboración entre entidades.
5. Que la información personal podrá ser transferida a otras entidades de certificación, dentro del marco de la Infraestructura Oficial de Firma Electrónica.

Asimismo, el titular declara lo siguiente:

1. Que conoce la responsabilidad que asume al utilizar su certificado de firma digital, equiparándola a su firma manuscrita.
2. Que todos los datos proporcionados son verdaderos y asume la obligación de notificar a la Entidad de Registro o sus puntos de verificación cualquier variación que los mismos puedan sufrir a lo largo del tiempo.
3. Que previo a la firma del presente documento no cuenta con inhabilitación o incapacidad declarada judicial o administrativamente, que lo limite en el ejercicio pleno de sus derechos.

De acuerdo al artículo 27.1 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos establece que “Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca.”

NOTA: Aquellos perfiles de certificados que no contengan al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal no podrán ser utilizados para la identificación y firma de las personas interesadas ante las Administraciones Públicas¹

Avisos legales

Declaración Responsable

El interesado manifiesta, bajo su responsabilidad, que los datos aportados en su solicitud son ciertos y que cumple con los requisitos establecidos en la normativa vigente para acceder a la pretensión realizada.

Datos Personales España

Los datos facilitados por Ud. en este formulario pasarán a formar parte de los archivos automatizados propiedad de la Entidad y podrán ser utilizados por el titular del archivo para el ejercicio de las funciones propias en el ámbito de sus competencias. De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Ud. podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición mediante instancia presentada. Lleidanet PKI SL utilizará sus datos para la prestación de los servicios de confianza de certificación digital, según se describe en la Declaración de Prácticas de Certificación lo que incluye, entre otros, la emisión y gestión de certificados digitales. En este proceso, Lleidanet PKI SL puede contar con la colaboración de autoridades de registro (RA) y de puntos de verificación presencial dependientes de las RA. Cualquier tercero podrá acceder a los datos que figuren en su certificado (a excepción de la clave privada) para comprobar la validez de los mismos. Lleidanet PKI SL no puede controlar el uso que los terceros hagan de sus datos por lo que no será responsable de ello en ningún caso. Lleidanet PKI SL tratará sus datos durante el tiempo que dure la prestación de servicios y, con posterioridad, durante el tiempo necesario para la gestión de certificados suspendidos o revocados y durante los plazos de tiempo legalmente previstos para la depuración de responsabilidades propias y de terceros.

¹ Administraciones Públicas en el ámbito subjetivo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas