



Firma digital. Marco legal, usos y retos.

Abog. Pedro Castilla del Carpio

24 de julio del 2025



Presidencia
del Consejo de Ministros





La Firma Electrónica y la Firma Digital (Ley 27269)

1

Firma Electrónica

Cualquier símbolo o dato creado con medios electrónicos que se usa con el propósito de autenticar un documento electrónico.

2

Firma Digital

Tipo especial de firma electrónica que usa tecnología de criptografía de doble clave para mayor seguridad.

a) Clave privada: Exclusiva del firmante y usada para firmar documentos.

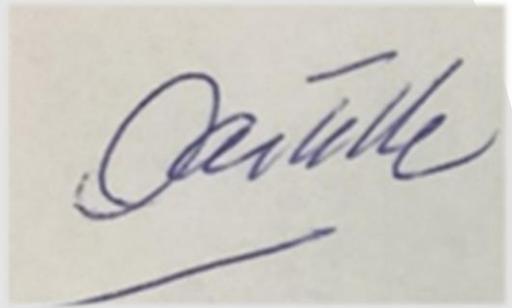
b) Clave pública: Sirve para verificar la autenticidad del documento.

3

Relación entre ellas

La firma digital es un tipo avanzado de firma electrónica, es decir, toda firma digital es una firma electrónica pero no toda firma electrónica es una firma digital. Se necesita de certificados digitales para su verificación.

Algunas modalidades de firma electrónica



FIRMA ESCANEADA
O DIGITALIZADA



FIRMA
DIGITAL



FIRMA DE
REGISTRO BIOMÉTRICO

FIRMA ELECTRÓNICA
MANUSCRITA



Cualquier firma electrónica puede tener efecto legal ... en la medida en que usted demuestre con evidencias el vínculo entre la firma y el presunto firmante.

La Firma Digital ... la más segura



Firma Digital

La firma digital es una modalidad de firma electrónica sustentada en mecanismos criptográficos. Si la firma digital se encuentra acreditada, se garantiza legalmente la autenticidad, la integridad y el carácter vinculante.

Tecnología que la sustenta

La encriptación electrónica que se utiliza para la firma digital es la misma que se usa en diversas aplicaciones, en Blockchain, en Whatsapp y en los portales web seguros ([https](https://)).

Facilidad de probanza

La tecnología de la encriptación electrónica empleada en la firma digital permite que la probanza del vínculo entre el firmante y el documento electrónico sea **inmediata**.

Certificado Digital

The screenshot shows a Windows-style dialog box titled "Certificado". The tabs at the top are "General", "Detalles" (which is selected), and "Ruta de certificación". The main content area has a title "Información del certificado" with an icon of a certificate. It contains the following text:

Este certif. está destinado a los siguientes propósitos:

- Protege los mensajes de correo electrónico
- Prueba su identidad ante un equipo remoto
- 1.3.6.1.4.1.5734.3.10.1
- 0.4.0.194112.1.0

* Para ver detalles, consulte la declaración de la entidad de certificación.

Emitido para: [REDACTED]

Emitido por: AC FNMT Usuarios

Válido desde 13/04/2020 **hasta** 13/04/2024

Tiene una clave privada correspondiente a este certificado.

Declaración del emisor

A large watermark "GEEKNETIC" is visible across the bottom of the screen.

El certificado digital contiene información con la cual los terceros pueden verificar si una firma digital es auténtica. Cada documento firmado digitalmente es enviado junto con el certificado digital del firmante. (Como si adjuntásemos el DNI a un contrato para que otros puedan verificar nuestra firma en el contrato).



Certificado Digital



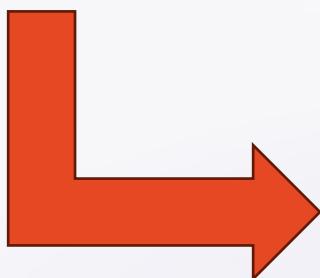
Documento Electrónico

Emitido por una Entidad de Certificación Digital (por ejemplo, RENIEC).



Clave Pública

Certifica la asignación de una **clave criptográfica pública** a una persona específica.



Identidad Digital

Funciona como un documento de identidad en entornos digitales.

Cada vez que usted firma y envía un documento electrónico, también su certificado es enviado. Se usará su data para verificar la autenticidad de su firma.

Screenshot of a digital certificate viewer application window titled "Certificado". The "Detalles" tab is selected. A dropdown menu shows "Mostrar: <Todos>". Below is a table of certificate fields:

Campo	Valor
Número de serie	01 00 00 00 00 01 27 86 1e 9f...
Algoritmo de firma	sha1RSA
Emisor	Akamai Subordinate CA 3, Aka...
Válido desde	Lunes, 22 de Marzo de 2010 0...
Válido hasta	Martes, 22 de Marzo de 2011 ...
Asunto	*.barnesandnoble.com, NEW ...
Clave pública	RSA (1024 Bits)
Puntos de distribución CRL	[1]Punto de distribución CRL: ...

Below the table is a large hex dump of the certificate's raw data:

```
30 81 89 02 81 81 00 ba 2a 55 07 b7 26 4d  
3c 4d b8 01 d6 70 7b a5 b0 bd 72 0d b8 e2  
c2 83 55 4a 24 64 58 8c ce f0 f2 0e af 97  
74 1c 10 9e 8b f3 6a 46 62 9a a8 94 c5 e1  
ef 10 d4 52 9d 73 80 61 5b 73 55 29 29 96  
89 a2 c5 a3 76 2e 9c 22 cb 95 cb ce f9 b7  
4e 88 15 34 ea a0 3c f1 cd ce 2e 6d 9b bd  
d2 72 42 f8 42 a1 41 8a c0 d4 ac a4 87 1b  
f4 a8 5c b9 b9 30 1e 74 af 54 e5 d7 e7 15
```

Buttons at the bottom include "Modificar propiedades...", "Copiar en archivo...", "Aceptar", and a small logo in the bottom right corner.

¿Qué es la IOFE?

Está constituida por:

1. Las empresas, entidades públicas y personas naturales acreditadas por el Indecopi.
2. Las políticas, estándares técnicos y lineamientos que ellas deben cumplir.
3. Los servicios que prestan y los productos que ofrecen vinculados a la tecnología de firma digital.

La suma de todo esto constituye el ecosistema digital de la **Infraestructura Oficial de la Firma Electrónica (IOFE)**.

Actores centrales



Es la Autoridad Administrativa Competente (AAC) que se encarga del otorgamiento y supervisión de las acreditaciones, 145 a la fecha, tanto a proveedores públicos como privados que generan productos y brindan servicios de firma digital.

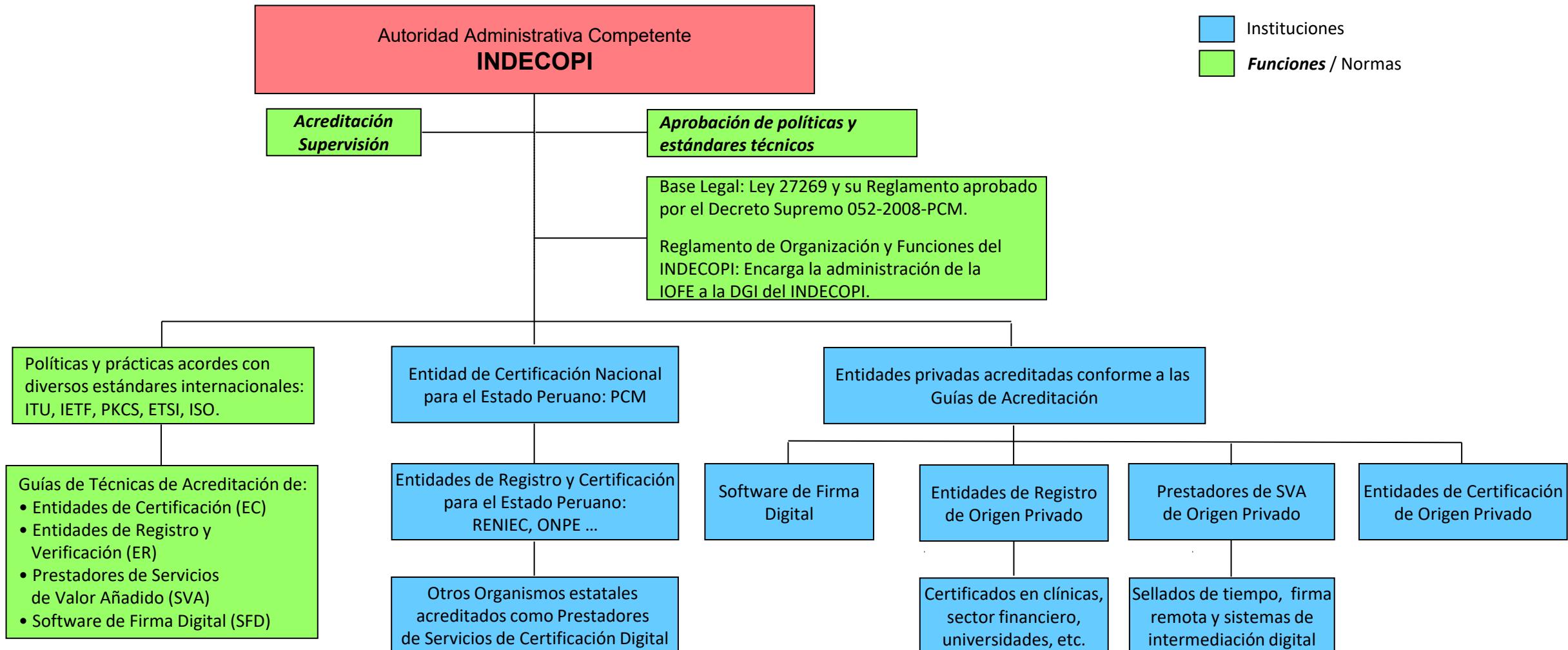


La PCM es la Entidad de Certificación Nacional para el Estado Peruano. Genera los certificados “raíz” para las demás entidades de certificación del Estado.



Es la Entidad de Certificación para el Estado Peruano que genera certificados digitales para los funcionarios públicos y el DNI electrónico para los ciudadanos.

Infraestructura Oficial de la Firma Electrónica



¿Qué es la Acreditación?

- En nuestro contexto, la acreditación es el reconocimiento de la Autoridad Administrativa Competente (**el Indecopi a través de la DGI**) de que una entidad privada o pública satisface los requerimientos técnicos y legales del Reglamento de la Ley de Firmas Digitales y de las Guías Técnicas de Acreditación para prestar los servicios solicitados asociados a la tecnología de firma digital dentro del marco de la Infraestructura Oficial de la Firma Electrónica.
- En el Perú, para prestar dichos servicios no es obligatorio haber obtenido la acreditación, pero contar con ella proporciona ventajas legales.
- La acreditación se obtiene luego de aprobar evaluaciones técnicas en las que se verifica el cumplimiento de los requisitos de la Guía Técnica de Acreditación correspondiente.
- Condiciones que debe cumplir la firma digital:
 - Haber sido generada con un software acreditado.
 - Ser *validable* con un certificado digital acreditado.



Presunciones legales en favor de la firma digital acreditada

Ventajas probatorias de la firma digital generada en la IOFE

1. En el caso particular de la firma digital acreditada, el Reglamento le confiere una “ventaja probatoria” que ni siquiera la firma manuscrita tiene.
2. Por las características de la tecnología que sirve de base a la generación de la firma digital, y que han sido verificadas por el Estado a través del proceso de acreditación, la probabilidad de que una firma digital sea falsificada es miles de veces menor a la probabilidad de que una firma manuscrita sea adulterada o falsificada.
3. Reconociendo este hecho, mediante el Reglamento de la Ley de Firmas y Certificados Digitales el Estado ha establecido que, ante un documento electrónico firmado digitalmente con software y certificado acreditados, se tendrá por autor al titular de dicho certificado digital, salvo prueba en contrario.
4. El Reglamento de la Ley de Firmas y Certificados Digitales establece la equivalencia funcional entre la firma manuscrita y la firma digital generada mediante servicios acreditados.

Presunciones legales sobre la Firma Digital acreditada.

Presunciones (Reglamento de Firmas Digitales, artículo 8):

- a) *“Que el suscriptor del certificado digital tiene el control exclusivo de la clave privada asociada.*
- b) *Que el documento electrónico fue firmado empleando la clave privada del suscriptor del certificado digital.*
- c) *Que el documento electrónico no ha sido alterado con posterioridad al momento de la firma”.*

Consecuencia:

“... el suscriptor no podrá repudiar o desconocer un documento electrónico que ha sido firmado digitalmente usando su clave privada ...”.





**APLICACIONES DE LOS
SERVICIOS Y PRODUCTOS
ACREDITADOS**

Plataforma de Facturación Electrónica SUNAT

Datos

1. No menos de 35,000 millones de documentos tributarios electrónicos, entre facturas, boletas de venta y otros comprobantes de pago electrónicos, firmados digitalmente y verificados mediante programas acreditados por el Indecopi (*).
2. La facturación electrónica se emplea a nivel mundial colaborando con el cumplimiento de las regulaciones fiscales, permitiendo así mejorar los servicios a los contribuyentes.
3. La SUNAT entrega a las MYPE certificados digitales tributarios gratuitos generados por el RENIEC, acreditados y auditados por el Indecopi, para que las MYPE puedan ingresar a la plataforma de facturación electrónica y firmar sus comprobantes de pago.

(*) Fuente: Portal de la SUNAT.



Ventanilla Única de Comercio Exterior (VUCE)

Ministerio de Comercio Exterior y Turismo

Datos

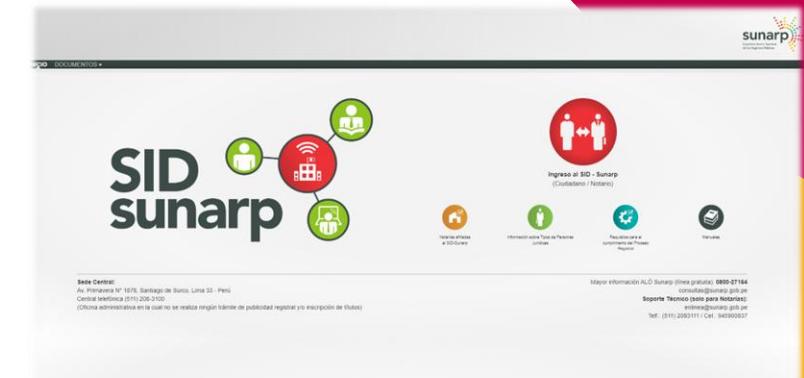
1. Importación o exportación de mercancías restringidas. Para iniciar el trámite electrónico, el interesado procede a su autenticación con su clave SOL de SUNAT (firma electrónica) o con su firma digital.
2. Certificados de origen: Garantizan el origen nacional del producto para que se le apliquen ventajas comerciales negociadas por el país. Para iniciar el trámite electrónico, el interesado procede a su autenticación con su clave SOL de SUNAT o con su firma digital.



Sistema de Intermediación Digital (SID) Superintendencia Nacional de Registros Públicos

El SID es una plataforma de servicios que permite realizar el procedimiento de inscripción registral a través de la presentación electrónica de documentos firmados digitalmente por un Notario. El SID recibe partes notariales de:

- Constitución de todas las modalidades de sociedades mercantiles. En Lima y Callao solo se aceptan firmadas digitalmente; *ya no en papel*.
- Otorgamiento de Poderes en el Registro de Personas Naturales. *En Lima y Callao sólo se aceptan en vía electrónica*. Disposición del DL Nº 1232, que modificó la Ley del Notariado.
- Compraventa de vehículos en el Registro Vehicular.
- Todos los actos inscribibles en el Registro de Sucesiones Intestadas.



DNI electrónico

Registro Nacional de Identificación y Estado Civil

Datos

1. El DNI electrónico contiene **dos** certificados digitales. Uno es para autenticar a la persona en forma remota y el otro sirve para generar, junto con un software, firmas digitales con equivalencia legal a la firma manuscrita y carácter legalmente vinculante.
2. El RENIEC es una de las Entidades de Certificación para el Estado Peruano. Como tal, ha sido acreditada por el Indecopi y es supervisada y auditada anualmente por la DGI.
3. Desde junio del 2024, se dejaron de emitir los DNI azules y amarillos.
4. Asimismo, desde esa fecha el acceso a consultas en línea de la ficha RENIEC sólo es posible mediante el DNI electrónico.



Sistema de Notificaciones Electrónicas (SINOE)

Expediente Judicial Electrónico (EJE)

Poder Judicial

Datos

1. El Sistema de Notificaciones Electrónicas (SINOE) y el Expediente Judicial Electrónico (EJE) utilizan certificados digitales y software de firma digital acreditados y supervisados por el Indecopi.
2. El SINOE permite recibir notificaciones judiciales en línea. El EJE permite la digitalización de la documentación de los procesos judiciales con el objetivo de mejorar el servicio de justicia, reduciendo los tiempos de tramitación y eliminando el uso de papel.

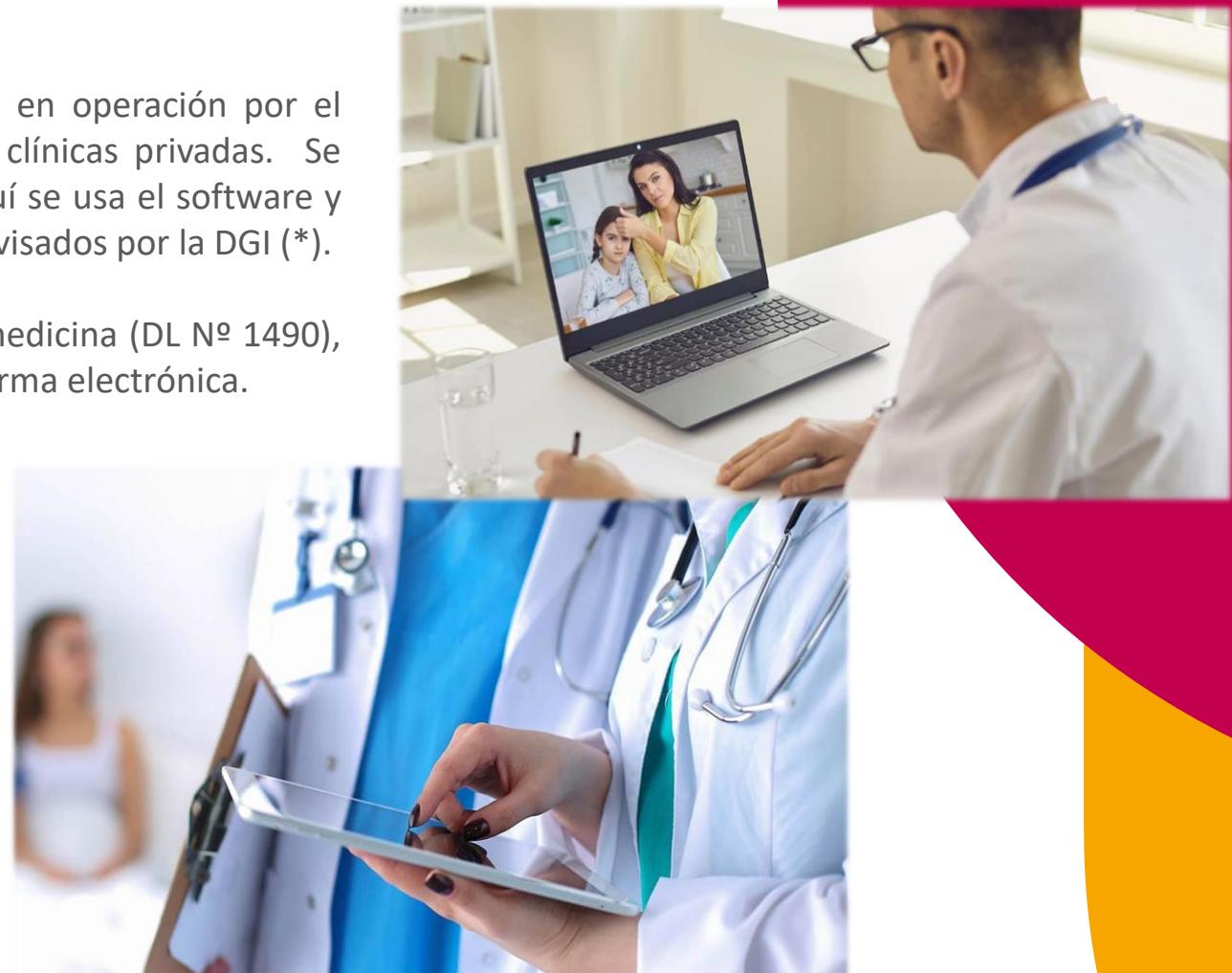


Telemedicina Sector Salud

Datos

1. Historias Clínicas Electrónicas. Las HCE han sido puestas en operación por el Ministerio de Salud, el Seguro Social de Salud y diversas clínicas privadas. Se tiene, aproximadamente, 14'000,000 de HCE. También aquí se usa el software y los certificados digitales acreditados por el Indecopi y supervisados por la DGI (*).
2. Telemedicina. Según la Ley del Fortalecimiento de la Telemedicina (DL Nº 1490), el consentimiento del paciente puede otorgarse mediante firma electrónica.

(*) Fuente: Portal Andina (15.12.2021)



Consultas frecuentes

1

¿Puede haber diferentes clases de firmas electrónicas en un mismo documento?

Es técnica y legalmente factible

3

Problemas con las versiones de los softwares de verificación de firmas digitales.

5

¿El Reniec entrega firmas digitales?

No. Entrega certificados digitales en el e-DNI

7

¿La clave que se solicita al firmar es la clave privada?

No

2

¿Cuántas veces se debe firmar un documento de numerosas páginas?

Una sola vez es suficiente

4

¿Se traslada el efecto legal desde el documento electrónico al documento físico?

No

6

¿Una firma digital garantiza la confidencialidad del contenido?

No, pero se puede usar la misma tecnología con ese fin.

8

¿Las firmas digitales generadas fuera del territorio peruano tienen equivalencia funcional con la firma manuscrita?

No



Acuerdo de Reconocimiento Mutuo (*)

El Acuerdo de Reconocimiento Mutuo es el documento suscrito por dos organismos de acreditación por el cual cada uno de ellos otorga a las entidades acreditadas por el otro los mismos derechos y obligaciones de las entidades acreditadas por sí mismo.

¿Qué se requiere para que una firma digital acreditada en el Perú pueda tener pleno efecto legal en otro país?

Es necesario:

- a) Que exista un Acuerdo de Reconocimiento Mutuo vigente entre el Perú y el otro país.
- b) Que el otro país esté representado por una entidad que cumpla funciones similares.
- c) Que los Acuerdos de Reconocimiento Mutuo garanticen en forma equivalente las funciones exigidas por la Ley y su Reglamento.

(*) Mención aparte: La certificación cruzada.

GRACIAS

www.gob.pe/Indecopi

Síguenos en: Indecopi Oficial

