

Obtención de firma y certificado digital

14 de mayo de 2020

La Ley N° 27269, Ley de Firmas y Certificados Digitales (la "Ley"), y su reglamento, aprobado mediante Decreto Supremo N° 052-2008-PCM ("Reglamento"), constituyen el marco normativo sobre la firma y certificado digital. Este régimen establece los mecanismos técnicos que permiten identificar al firmante y acreditar su voluntad en las operaciones electrónicas bajo un entorno de seguridad y validez.

A. CONCEPTOS SOBRE LA FIRMA Y CERTIFICADO DIGITAL

La Ley y el Reglamento establecen que la firma digital es una modalidad de firma electrónica que utiliza una técnica de criptografía asimétrica,¹ basada en el emparejamiento de claves (privada y pública) que permite vincular al signatario con el documento electrónico. Es importante mencionar que la firma digital no es una reproducción de la firma gráfica manuscrita, sino que es una secuencia numérica resultante del proceso criptográfico antes indicado y que es generado a partir de certificados digitales.

Los certificados digitales son las credenciales electrónicas generadas y firmadas digitalmente por una Entidad de Certificación que vincula un par de claves (privada y pública) con una persona natural o jurídica, confirmando de esta manera su identidad. El certificado digital contiene la clave pública, la cual permite descifrar los datos al destinatario del documento para comprobar la identidad del firmante.

La firma digital tiene la misma validez y eficacia jurídica que el de una firma manuscrita, siempre que haya sido generada por un Prestador de Servicios de Certificación Digital ("PSCD") debidamente acreditado y dentro de la Infraestructura Oficial de Firma Electrónica (la "IOFE"). Ello implica que, los documentos electrónicos firmados digitalmente dentro del marco de la IOFE deberán ser admitidos como pruebas en los procesos judiciales y/o procedimientos administrativos.

El uso de la firma y certificado digital permiten garantizar: (i) la autoría del documento electrónico; (ii) su integridad, dado que certifica que el documento no ha sido alterado desde su emisión; y, (iii) evita el rechazo del documento, es decir, que el firmante desconozca la autenticidad del documento firmado.

B. OBTENCIÓN DEL CERTIFICADO DIGITAL

La IOFE se encuentra conformada, entre otros, por las Entidades Certificadoras y de Revisión. Las Entidades Certificadoras cumplen la función de emitir o cancelar los certificados digitales, así como brindar los servicios inherentes al propio certificado; mientras que las Entidades de Revisión se encargan de identificar a los titulares y/o suscriptores del certificado digital y aprobar o denegar las solicitudes de emisión de certificados digitales. Una Entidad Certificadora puede ser a la vez una Entidad de Registro.

Las Entidades Certificadoras y de Registro que pertenecen al IOFE pueden ser visualizadas a través del siguiente link:

<https://www.indecopi.gob.pe/en/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl->

Las personas naturales y/o jurídicas que deseen obtener un certificado digital para poder firmar electrónicamente un documento, deberán dirigirse a una Entidad Certificadora o de Registro acreditada ante el Instituto de Defensa de la Competencia y de la Protección de la Propiedad Intelectual ("INDECOPI"), los cuales constan en la página web antes descrita.

Si bien los requisitos exigidos entre las distintas entidades pueden variar, por lo general se requerirán

¹Según el Reglamento, la criptografía asimétrica es la rama de las matemáticas que emplea algoritmos para convertir un mensaje legible en un texto incomprensible y luego devolverlo a su forma original. La criptografía asimétrica emplea dos claves diferentes pero relacionadas entre sí. Por un lado, una clave permite cifrar el mensaje (esta es la clave privada y secreta) y; por otro lado, la otra clave permite descifrarlo. Esta última es necesariamente de conocimiento público

presentar los siguientes documentos para obtener un certificado digital:

a. PERSONA NATURAL:

- i) Formulario de solicitud (en el cual se requiere información respecto a la identidad de la persona); y,
- ii) Copia del Documento Nacional de Identidad.

b. PERSONA JURÍDICA:

- i) Formulario de solicitud (en el cual se requiere información respecto a la identidad de la persona jurídica);
- ii) Ficha RUC de la persona jurídica;
- iii) Copia del Documento Nacional de Identidad del representante legal de la persona jurídica;
- iv) Copia de la vigencia de poder del representante legal de la persona jurídica;
- v) Indicar quién será la persona natural suscriptora del certificado digital (el suscriptor); y,
- vi) Copia de del Documento Nacional de Identidad del suscriptor.

Las Entidades Certificadoras y de Registro deberán validar de manera previa la identidad de los titulares y suscriptores de los certificados digitales (generalmente, de manera presencial). Sin embargo, en el contexto actual del estado de emergencia sanitaria el INDECOPI ha exceptuado de manera excepcional de dicha validación presencial, siendo necesario cumplir únicamente con la documentación solicitada².

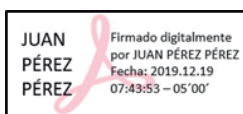
Los costos promedios por obtención de certificados digitales oscilan entre los US\$ 50.00 (cincuenta y 00/100 Dólares de los Estados Unidos de América) a US\$ 80.00 (ochenta y 00/100 Dólares de los Estados Unidos de América) de manera anual, por cada titular y/o suscriptor. Asimismo, los costos dependerán de los años de vigencia del certificado.

C. ¿CÓMO FUNCIONA EL CERTIFICADO DIGITAL?

- 1. Una vez solicitado el certificado digital, las Entidades Certificadoras procederán a registrarlo y enviarán a cada titular y/o suscriptor el certificado correspondiente.
- 2. Con asesoría del personal de las Entidades Certificadoras, los titulares y/o suscriptores procederán a instalar lo certificados digitales en las computadoras.
- 3. Al instalar los certificados digitales, se consignará una clave privada asociada al certificado.
- 4. Los certificados digitales deberán configurarse en los programas a través de los cuales se trabajarán los documentos electrónicos; es decir, Microsoft Word, Microsoft Excel, Adobe Acrobat Reader, entre otros.
- 5. Culminada la instalación, los titulares y/o suscriptores podrán insertar las firmas digitales, generadas a partir de los certificados digitales, en los documentos electrónicos.

Cabe señalar que los certificados digitales quedarán instalados en las computadoras que se usen para tal fin, por lo que se recomienda que esta sea de uso personal.

A modo de ejemplo, una firma digital quedará insertada en un documento electrónico de la siguiente manera:



² Comunicado del INDECOPI: INDECOPI flexibiliza requisitos para quienes necesiten obtener certificados digitales por primera vez. En: <https://www.indecopi.gob.pe/en/-/la-comision-para-la-gestion-de-la-infraestructura-oficial-de-firma-electronica-flexibiliza-requisitos-para-qui-ienes-necesiten-obtener-certificados-digi>

Para comprobar la validez de la firma digital, el destinatario podrá hacer clic en esta y apreciar el certificado digital de la siguiente manera:

