



Libro blanco

Firma Electrónica

en República Dominicana



Asociación Dominicana
de Empresas FinTech

Control del documento



Permitida la reproducción o distribución del presente documento citando al autor e incluyendo un enlace al artículo original.

Versión	Descripción	Autor	Revisado por
1.0	Documento inicial, 25 de junio, 2020	AdoFinTech: Inés Páez, Directora Ejecutiva	<ul style="list-style-type: none"> ▪ INDOTEL: José Raúl Madera Encargado Dpto. Firma Digital ▪ Avansi: Carlos Gómez Gerente General ▪ CCPSD: Iván Santana Consultor Soluciones Digitales ▪ OMG: Natachú Domínguez Directora Senior de Administración de Conflictos ▪ Pellerano & Herrera: Alessandra Di Carlo Socia Práctica Corporativa

Santo Domingo, República Dominicana
www.adofintech.org | hola@adofintech.org

Contenido

- 4** Introducción
- 5** Firma electrónica en 1 página
- 6** ¿Qué es la firma electrónica?
- 7-8** Marco legal en República Dominicana
- 9** Rol del Indotel en torno a la firma electrónica
- 10** Tipos de firmas electrónicas
- 11-12** ¿Quiénes están autorizados a emitir firma electrónica?
- 13** Beneficios de la firma electrónica
- 14** Posibles casos de uso del certificado digital
- 15** Comprobantes fiscales electrónicos (e-CF)
- 16** La firma electrónica en el Poder Judicial
- 17-20** Jornada de uso:
 - ¿Qué hacer para tener una firma electrónica?
 - ¿Cómo se usa una firma electrónica?
 - ¿Cómo válido una firma en un documento?
- 21** Referencias bibliográficas
- 22** Agradecimientos

Introducción

Al momento de constituir ADOFINTECH definimos varios lineamientos estratégicos que guiarían nuestras actividades, entre ellos, apoyar el desarrollo de las nuevas tecnologías.

La cantidad de documentos que firmo diariamente y que necesitan ser archivados son motivo para migrar a una vida sin papeles, “*paperless*”, que se apoye precisamente en las nuevas tecnologías que nos permitan mantener los parámetros de seguridad que le den la garantía a nuestras firmas en el mundo digital.

Este libro blanco tiene el objetivo de informar a las personas y empresas sobre la implementación de la firma electrónica, como forma de simplificar y agilizar los procesos administrativos de su cotidianidad. Contiene una explicación sobre la firma electrónica, sus variantes y otros conceptos básicos vinculados a ella, cubriendo el paso a paso de su uso y validación. Quisimos también incluir referencias a las normativas locales e internacionales, de manera que el lector entienda el marco legal que avala este instrumento.

Sin duda alguna, la firma electrónica está ganando terreno en el país y a nivel mundial, gracias a sus múltiples beneficios, razón por la cual apostamos a ella, viendo que cada día son más los casos de uso y escenarios donde puede traer ahorros de tiempo y recursos.

Me gustaría dar las gracias a todos los que han colaborado en la elaboración y revisión de este documento, que estoy seguro será una guía importante para quienes necesiten profundizar en este tema.

Manuel A. Grullón Hernández

Presidente de la Asociación Dominicana de Empresas de Fintech
Junta Directiva 2019-2020

Firma electrónica en 1 página

Firma Electrónica

La **firma electrónica** ofrece una manera de firmar documentos digitales, de forma similar a como firmamos un documento en el mundo físico. Se usa con la intención de manifestar la aprobación o el consentimiento de la información contenida en un documento.

¿Para qué sirve?



Identificar a la persona que firma



Integridad: que el documento original no se ha modificado después de su firma



Control del firmante: Evitar fraude o la negación de un documento ya firmado.

Certificado Digital

Una firma electrónica es un archivo de datos llamado **"certificado cualificado de firma electrónica"** * que se adjunta a un documento electrónico, identificando a la persona que firma (o el rol que ocupa en una institución), a través de medios digitales, para que quede constancia de que esa persona firmó ese documento.

* Debe ser emitido por una **Entidad de Certificación**.

Tipos de firmas electrónicas



Firma electrónica simple



Firma electrónica avanzada



Firma electrónica cualificada

Marco legal

- **Ley 126-02** sobre comercio electrónico, documentos y firma digital
- **Decreto 335-03** que aprueba el Reglamento general de aplicación de la ley 126-02
- **Resolución núm. 071-19** emitida por el Indotel, que dicta las normas complementarias



Beneficios

- ✓ Garantía, seguridad e integridad de la información
- ✓ Eficiencia y productividad
- ✓ Reducción de costos
- ✓ Fortalece la imagen empresarial
- ✓ Cuida el medioambiente

¿Cómo se usa?

Se puede firmar con certificado digital usando distintas herramientas:



Visor de PDF



Gestor de correo electrónico



Aplicaciones móviles



Portafirmas



Motor de firma



Desde la nube

Posibles casos de uso

- Comercio
- Sector financiero
- Sector Inmobiliario
- Sector asegurador

Perfeccionamiento de Garantías en General:

- Procesos judiciales
- Administración pública
- Adm. empresarial

¿Dónde la solicito?



Asociación Dominicana de Empresas FinTech



Firma Electrónica

¿Qué es?

Muchas personas tienen la idea errónea de que la firma electrónica es la firma manuscrita escaneada, pero no es así.

La firma electrónica ofrece una manera de firmar documentos digitales, con un valor similar al que logramos cuando firmamos un documento en el mundo físico. Una firma electrónica es un archivo de datos en un formato digital que se adjuntan a un documento electrónico de manera lógica, y es aplicada o utilizada por una persona con una intención de firmar como prueba de la aprobación o el consentimiento de la información contenida en el documento.

Una firma electrónica puede tener tanto valor como la versión manuscrita y cumplir con las mismas funciones, siempre que cumpla con determinados requisitos. A saber:

- 1. Identidad:** poder identificar a la persona que firma o firmante,
- 2. Integridad:** validar o garantizar la integridad del documento original firmado, es decir, que no ha sido modificado después de su firma,
- 3. Control sobre el firmante:** evitar intentos de fraude, de suplantación de identidad o negación de un documento ya firmado.

La firma electrónica avanzada se crea utilizando un archivo de datos llamado “certificado cualificado de firma electrónica”, el cual se genera mediante procesos matemáticos y criptográficos de alta seguridad, y cuenta con dos claves, una pública y la otra privada, que solo conoce el propietario de la misma; la clave pública es avalada por los mecanismos de seguridad que el INDOTEL le exige a las entidades Prestadoras de Servicios de Confianza Cualificados que las emiten y caduca con el tiempo.

Certificado digital

Es el archivo digital que se emite para garantizar que una persona o empresa es quien dice ser, y que al utilizar dicho certificado le permite firmar documentos o mensajes electrónicos para validar el contenido de los mismos, mientras dure su período de vigencia.

NOTA: La Resolución No. 071 del Indotel, con el fin de adaptar nuestra normativa a los criterios y prácticas internacionales sobre el tema, estableció la equivalencia entre el término de “firma digital” (definida inicialmente en la Ley No. 126-02) y la “firma electrónica cualificada” (la “firma electrónica”). De igual manera, se dispuso la equivalencia entre la “Entidad de Certificación” (definida inicialmente en la Ley No. 126-02) y las entidades Prestadora de Servicios de Confianza Cualificados.

En consecuencia, en el presente documento nos referiremos de manera unificada a la firma electrónica (equivalente a firma digital), a la Entidad de Certificación (equivalente a Prestadora de Servicios de Confianza Cualificados) y abreviaremos como “certificado digital” al “certificado cualificado de firma electrónica”.

2002

Ley 126-02 sobre comercio electrónico, documentos y firma digital.
De fecha 4 de septiembre de 2002.

2003

Decreto 335-03 que aprueba el Reglamento general de aplicación de la Ley 126-02.

2004

Resolución 010-04 mediante la cual se aprueban las normas complementarias a la Ley 126-02, incluye: especificaciones tecnológicas aplicables a los certificados, políticas y procedimientos de certificación, autorización y acreditación; además de criterios de seguridad y auditoría.

2006

Resoluciones>> 026-06: relativa a la determinación de la hora en medios electrónicos e internet; **043-06:** sobre Publicidad y Difusión de Información de los Consumidores y Usuarios por los Sujetos Regulados; **055-06:** sobre Protección de Datos de Carácter Personal por los Sujetos Regulados; **094-06:** sobre la actualización de los valores de los costos, derechos y multas aplicables a las entidades reguladas; **113-06:** sobre el monto de la fianza o seguro de responsabilidad que deben contratar las entidades que soliciten ser acreditadas como entidad de certificación; **129-06:** Que aprueba la Norma de Calidad de Servicio y Seguridad de la Red; **142-06:** relativa a La Protección de los Derechos de los Consumidores y Usuarios; **166-06:** Que conoce la solicitud de autorización presentada por la sociedad comercial **Avansi, C. por A.**, para operar como entidad de certificación y prestar los servicios de certificación digital.

2007

Resoluciones>> 033-07: sobre el Uso de Mensajes de Datos, Documentos y Firmas Digitales en los Medios de Pagos Electrónicos; **169-07:** Que conoce la solicitud de autorización presentada por la **Cámara de Comercio y Producción de Santo Domingo, Inc.** Para operar como entidad de certificación y prestar los servicios de certificación digital.

2009

Resolución 035-09: que aprueba la norma complementaria, para la Integración de la Jurisdicción Inmobiliaria en la Infraestructura de Firma Digital Nacional.

2011

Resolución 025-11: Firmas Digitales, a los procedimientos aduaneros.

2013

Resolución 041-13: Norma sobre el Uso de Mensajes de Datos, Documentos y Firmas Digitales en los Medios de Pagos Electrónicos.

2018

Resolución 024-18: que conoce la solicitud de autorización presentada por la Oficina Presidencial de Tecnologías de Información y Comunicación (**OPTIC**) para operar como Entidad de Certificación.

2019

Resolución núm. 071-19, que dicta la norma complementaria por la que se establece la equivalencia regulatoria del sistema dominicano de infraestructura de claves públicas y de confianza con los marcos regulatorios internacionales de servicios de confianza y la norma complementaria sobre procedimientos de autorización y acreditación.
Esta norma comprende las disposiciones normativas relacionadas a los Criterios de Auditoría, Estándares Tecnológicos, Políticas y Procedimientos de Certificación y Procedimientos de Seguridad.

2020

Resolución 35-20, que contiene la Norma de Aplicación de la Ley Núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales a los Procedimientos Tributarios. Esta norma está alineada al Código Tributario, así como a normas relacionada con el Uso de Medios Telemáticos de la DGII y sobre el Comprobante Fiscal Electrónico (e-CF).

¿La firma electrónica es reconocida internacionalmente?

La firma electrónica tiene valor legal en la mayoría de los países del mundo. Aunque no exista un marco legal unificado a nivel global, casi todas las leyes en los demás países están alineados a los mismos criterios definidos por la Comisión de las Naciones Unidas para el Derecho Mercantil (UNCITRAL). Recomendamos validar la normativa o regulación del país donde se va a ejecutar el documento a firmar, a los fines de asegurar que reconozcan la validez de los certificados emitidos por entidades de certificación extranjeras.

Fundamento internacional

El **artículo 14** del **Reglamento eIDAS** (Reglamento de la Unión Europea No. 910/2014), señala que los servicios de confianza prestados por los prestadores en un tercer país, **serán reconocidos** como legalmente equivalentes a los servicios prestados por prestadores establecidos en la Unión Europea, si los servicios de confianza originarios del tercer país son reconocidos en virtud de un acuerdo celebrado entre la Unión y el tercer país en cuestión u organizaciones internacionales de conformidad con el **artículo 218** del **Tratado de Funcionamiento de la Unión Europea**.

Acuerdo Asociación Económica CARIFORUM-CE ofrece la cobertura legal para el cumplimiento del artículo 14 b) del **Reglamento eIDAS** relativo al reconocimiento de la equivalencia entre los servicios ofrecidos por prestadores dominicanos y prestadores establecidos en la **Unión Europea**.

El **Tratado del CARIFORUM-CE**, en su **Artículo 120**, dispone el reconocimiento mutuo de certificados electrónicos entre países intervinientes en este Tratado; así como la posibilidad de intercambiar información de su legislación y sobre la aplicación de estas.

Actualmente, las Naciones Unidas trabajan el Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza.



“Vivimos una nueva realidad a la cual las empresas deben responder, y es necesario simplificar los procesos de los clientes. La implementación de la firma electrónica apoya esta transición, además reduce costos, acorta tiempos y aumenta la seguridad.”

Jorge Mancebo
Presidente de Sendiu

La Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales, en el Artículo 56, establece que el Instituto Dominicano de las Telecomunicaciones (INDOTEL) ejercerá la función de **entidad de vigilancia y control de las actividades desarrolladas por las entidades de certificación**. Tendrá, en especial, las siguientes funciones:

1. Autorizar, conforme a la reglamentación expedida por el Poder ejecutivo, **la operación de entidades de certificación** en el territorio nacional;
2. Velar por el **adecuado funcionamiento y la eficiente prestación del servicio** por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad;
3. **Efectuar las auditorías** de que trata la Ley núm. 126-02;
4. Definir reglamentariamente los **requerimientos técnicos** que califiquen la idoneidad de las actividades desarrolladas por las entidades de certificación;
5. Evaluar las actividades desarrolladas por las entidades de certificación autorizadas conforme a los requerimientos definidos en los reglamentos técnicos;
6. Revocar o suspender la autorización para operar como entidad de certificación;
7. Requerir en cualquier momento a las entidades de certificación para que suministren información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren;
8. **Imponer sanciones a las entidades de certificación por el incumplimiento** o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio;
9. Ordenar la revocación o suspensión de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales;
10. Designar los repositorios y entidades de certificación en los casos previstos en la ley;
11. **Proponer al Poder Ejecutivo la implementación de políticas** en relación con la regulación de las actividades de las entidades de certificación y la adaptación de los avances tecnológicos para la generación de firmas digitales, la emisión de certificados, la conservación y archivo de documentos en soporte electrónico;
12. **Aprobar los reglamentos internos de la prestación del servicio**, así como sus reformas;
13. Emitir certificados en relación con las firmas digitales de las entidades de certificación,
14. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas en los mercados atendidos por las entidades de certificación.



Firma electrónica simple

Nombre anterior en Ley 126-02: Firma electrónica

La firma electrónica simple es realizada a través de un medio electrónico y su uso debe ser acordado entre las partes. Esta sirve para que el cliente o usuario demuestre su conformidad con el contenido de un documento o contrato. Son los datos en formato electrónico agregados a otros, o asociados de manera lógica con aquellos que utiliza el firmante para firmar.



Firma electrónica avanzada

Nombre anterior en Ley 126-02: Firma Digital

Es una firma electrónica que cumple los siguientes requisitos:

- Relacionada de forma única a quien firma
- Permite identificar al firmante
- Ser creada usando un certificado digital con alto nivel de confianza, bajo uso exclusivo del firmante
- Vinculada al documento firmado de forma que cualquier modificación posterior a la firma sea detectable.

Requieren
el uso de un
**Certificado
Digital**



Firma electrónica cualificada

Nombre anterior en Ley 126-02: Firma Digital Segura

Es una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica emitido por un Prestador de Servicios de Confianza (PSC).

Nota: Los tres tipos de firmas electrónicas son válidas y legales. Sin embargo las firmas electrónica avanzada y cualificada al usar un certificado digital brindan mayor nivel de seguridad porque facilitan la identificación del firmante y permite garantizar la integridad del documento.

Tipos de Certificados Digitales

- **Local:** Se descarga e instala en el dispositivo electrónico y la firma solo podrá realizarse desde el equipo en el que el certificado se encuentra instalado. Tiene dependencia del dispositivo, por lo que si se extravía o lo roban, se deberá solicitar la revocación o cancelación del mismo, y luego solicitar la generación de un nuevo certificado digital.
- **En la nube:** Se encuentra almacenado en la nube en un servidor criptográfico con ciertas características. Permite al firmante acceder desde cualquier ordenador o dispositivo móvil. Limita los riesgos a nivel de seguridad, porque requiere credenciales para poder utilizarse y elimina la dependencia de un dispositivo electrónico.



Prestador Cualificado de Servicios de Confianza

Son las entidades que ofrecen uno o varios servicios de confianza cualificados y que están autorizados y validados por el INDOTEL, estos son:

Entidad de Certificación

Es la entidad responsable de la **emisión, y gestión de los certificados digitales**. Actúa como tercera parte de confianza, entre el firmante y la persona que confía en las relaciones electrónicas.

Una entidad de certificación está autorizada para emitir certificados de firmas digitales, ofrecer o facilitar los servicios de registro y estampado cronológico de tiempo de la transmisión y recepción de documentos digitales, mensajes de datos, operaciones y transacciones electrónicas, así como otras funciones relativas a las soluciones basadas en firmas digitales.

Unidades de Registro

Son las entidades autorizadas por el INDOTEL, para asistir a las Entidades de Certificación en la gestión de las solicitudes, **validando los datos de identidad y registro de los solicitantes** de certificados digitales.

También están en capacidad de ofrecer otros servicios de validación relacionados con las firmas digitales.
En inglés, Registration Authority (RA).



* Autorizada mediante la Resolución núm. 166-06 de fecha 28 de septiembre de 2006



* Autorizada mediante la Resolución núm. 169-07 de fecha 23 de agosto de 2007



* Autorizada mediante la Resolución núm. 020-16 del Consejo Directivo



* Autorizada mediante la Resolución núm. 008-18 del Consejo Directivo



* Autorizada mediante la Resolución núm. 024-18 de fecha 6 de junio de 2018

* La Dirección General de Impuestos Internos también está autorizada como Unidad de Registro mediante la Resolución núm. 049-13 del Consejo Directivo.

Entidades de certificación y tipos de certificados digitales



AVANSI

Cámara Santo Domingo (CCPSD)

OPTIC

Certificado de Firma para Persona Física

Certificado de Persona Física Individual:

- Formulario completado
- Cédula/Pasaporte

Validez: 2 años

Precio: emisión 2,360 pesos / renovación: 1,180 pesos

Certificado de Firma Digital Personal:

- Formulario completado
- Cédula/Pasaporte

Validez: 2 años

Precio: 45 USD

Certificados de Ciudadano:

- Formulario completado
- Cédula/Pasaporte

Validez: 1 año

Certificado de Firma para Empresas o Gobierno

Certificados Corporativos:

- Formulario autorización completado
- Cédula/Pasaporte del representante autorizado que solicita
- Cédula/Pasaporte del empleado titular del certificado
- RNC
- Registro Mercantil (si aplica)

Validez: 2 años

Precio: emisión 2,360 pesos / renovación: 1,180 pesos

Certificado de Firma Digital Empresarial o Gubernamental:

- Formulario autorización completado
- Cédula/Pasaporte del representante autorizado que solicita
- Cédula/Pasaporte del empleado titular del certificado

Validez: 2 años

Precio: 45 USD

Certificado de Firma Digital Gubernamental

- Solicitud formal firmada por el representante de la institución y dirigida al Director General de la OPTIC
- Formulario autorización completado
- Cédula/Pasaporte del representante autorizado que solicita
- Certificación laboral en papel timbrado de cada empleado solicitante, firmada y sellada
- Cédula/Pasaporte del empleado titular del certificado
- Carta de autorización del supervisor inmediato

Validez: 1 año

AVANSI

Filial del Grupo Viafirma

www.viafirma.do/

Tel.: 809-682-3928

unidadregistro@avansi.com.do

Avenida Lope de Vega No. 19
Edificio PIISA A, suite 102, Naco
Santo Domingo, Distrito Nacional

Cámara Comercio y Producción de Santo Domingo

Soluciones Digitales | DIGIFIRMA
camarasantodomingo.do/digifirma/

Tel.: 809-682-2688, opc.4

digifirma@camarasantodomingo.do

Avenida 27 de febrero No. 228
Edificio Friusa, La Esperilla
Santo Domingo, Distrito Nacional

Oficina Presidencial de Tecnologías de la Información y Comunicación **OPTIC**

optic.gob.do/firma-digital/

Tel.: 809-286-1009

firmadigital@optic.gob.do

Avenida 27 de febrero No. 419 casi esq.
Núñez de Cáceres
Santo Domingo, Distrito Nacional



Para persona física

Para empresas

Eficiencia y productividad



- ✓ Puede ser utilizada sin la presencia física.
- ✓ Reduce los tiempos de respuesta, y ofrece mejor control y monitoreo de los trámites.

- ✓ Conlleva un ahorro de tiempo en firmar documentos y procesos de gestión relacionados, que representa una optimización de los recursos.

Reduce costos



- ✓ Firmar desde cualquier lugar y cualquier momento.
- ✓ Menos filas y tiempo invertido en realizar gestiones de documentos.

- ✓ Reduce los costos relacionados a la impresión de documentos: menos consumo de papel, de tinta, de gastos en mantenimiento de impresoras, de archivo y de gestión de documentación.

Garantía



- ✓ Seguridad e integridad de la información.

- ✓ Se crea por medios que están bajo el control del firmante, tanto el dispositivo electrónico como la llave privada.
- ✓ Es posible detectar cualquier cambio que se realice en el documento después de haber sido firmado.
- ✓ Cuando es cualificada, ofrece mayor cobertura legal y menores riesgos que la firma tradicional.

Fortalece la imagen empresarial



- ✓ Experiencia mejorada de los clientes, haciendo los trámites más simples y mejorando tiempos de respuesta.

- ✓ El uso de este tipo de tecnologías mejora la reputación de las empresas de forma positiva: imagen de innovación, facilitando los procesos internos y logrando mayor satisfacción de los empleados.

Cuida el medioambiente



- ✓ Al reducir el consumo de papel contribuimos a proteger el planeta disminuyendo el impacto ambiental.

Posibles casos de uso en los que se pudiera utilizar la firma electrónica*:



Sector financiero:

- Firma de créditos hipotecarios y préstamos personales
- Apertura de cuentas bancarias
- Solicitud de tarjetas de crédito
- Apertura de cuentas de corretaje en el mercado de valores



Comercio:

- Firma de contratos
- Pagos por bienes
- Aceptación de servicios



Empresariales

- Pago de nóminas
- Extensiones de contrato, y aumentos de salario
- Contratos de trabajo



Procesos judiciales:

- Denuncias y demandas
- Cesión de poderes
- Expedientes electrónicos



Sector Inmobiliario:

- Notificaciones legales
- Testamentos, cesiones, venta o alquiler



Sanidad:

- Firma de pólizas de seguro
- Autorizaciones de procedimientos médicos
- Tasaciones de siniestros



Adm. Pública & Regulatorio:

- Solicitudes de servicios
- Certificación de documentos
- Remisión de documentación oficial

** Estos son casos ilustrativos de los usos que pudiera tener la firma electrónica, aunque todavía en la República Dominicana, no todas las instituciones ni las empresas del sector privado reconocen el instrumento o documento como válido cuando contiene firma electrónica.*



“En el caso del factoring y confirming sin firma electrónica habría que hacer todos los procesos de manera presencial.

La firma electrónica es la base de nuestra operaciones, reduciendo costos y tiempo, facilita hacer operaciones con empresas en el interior del país sin trasladarse.”

Miguel Ángel Adames,
Gerente General de Mercofact



La Resolución 35-20, que contiene la Norma de aplicación de la Ley 126-02 a los procedimientos tributarios, tiene el fin de simplificar los trámites y agilizar los mismos mediante la utilización de documentos digitales, en consonancia con las buenas prácticas internacionales en la materia.

Esta norma está alineada al Código Tributario, así como a normas relacionada con el Uso de Medios Telemáticos de la DGII y sobre el Comprobante Fiscal Electrónico (e-CF).

¿Qué es un Comprobante Fiscal Electrónico (e-CF)?

Es un comprobante fiscal que se emite, firma y recibe electrónicamente acreditando la transferencia de bienes, entrega en uso o la prestación de servicios, debiendo cumplir siempre con los requisitos establecidos en el **Decreto núm. 254-06**.

Características de un e-CF:

- Tiene validez y efectos legales iguales a la factura en papel.
- Se emite electrónicamente
- Tiene un formato estándar de factura
- **Firmado digitalmente**
- Tiene una mayor seguridad e integridad de la información

Los **tipos de comprobantes fiscales electrónicos** son codificados y nombrados de la siguiente forma:

- Factura de Crédito Fiscal Electrónica
- Factura de Consumo Electrónica
- Nota de Crédito Electrónica
- Nota de Débito Electrónica
- Compras Electrónico
- Gastos Menores Electrónico
- Regímenes Especiales Electrónico
- Gubernamental Electrónico
- Exportación Electrónico
- Pagos al Exterior Electrónico

En adición, estos comprobantes (e-CF) estarán diferenciados de los comprobantes fiscales usados para facturar en papel, por tener secuencias que inician con la serie E, seguido del tipo de e-CF y un secuencial de 10 dígitos, manteniendo la siguiente estructura:

Serie Secuencial

E310000000001

Tipo de e-CF

¿Quiénes emiten e-CF?

Emiten e-CF los contribuyentes que previamente hayan sido autorizados por Impuestos Internos.

Para emitir un e-CF los emisores electrónicos utilizan un software de facturación que permite generar la factura en el formato estándar XML y según las especificaciones técnicas de Impuestos Internos. Dicho software es diseñado o adquirido por el contribuyente, de acuerdo con las necesidades de su actividad comercial.

Requisitos para emitir e-CF

Para facturar electrónicamente, los contribuyentes deben cumplir con los siguientes requisitos:

1. Estar inscritos en el Registro Nacional de Contribuyentes (RNC).
2. Tener autorización para emitir comprobantes fiscales.
3. Estar al día en el cumplimiento de sus obligaciones tributarias.
4. Disponer de **certificado digital para procesos tributarios**, emitido por una prestadora de servicios de confianza (entidad de certificación) que corresponda a la persona que actuará en representación del contribuyente.
5. Disponer de un software para la emisión de Comprobantes Fiscales Electrónicos (e-CF), el mismo puede ser desarrollado por su empresa o adquirido a través de un proveedor de software de facturación electrónica certificado por DGII.
6. *Adicional, en caso de ser proveedor de software, la actividad económica debe estar relacionada con la venta y/o desarrollo de aplicaciones informáticas.*

Consulta de e-CF

El estatus de un e-CF puede ser verificado, una vez ha sido recibido en Impuestos Internos, a través de la consulta disponible en el portal web de Impuestos Internos (www.dgii.gov.do)

El código QR de la representación impresa permite consultar el estatus y la validez de un e-CF, e indicará los estados "Aceptado", "Rechazado" y "No encontrado", según correspondan.

Todo emisor electrónico deberá entre otras responsabilidades: incorporar su Certificado Digital vigente en todos los e-CF emitidos, y emitir la representación impresa del e-CF cuando así lo requiera un receptor no electrónico.

El Consejo del Poder Judicial aprobó, en su sesión ordinaria 014-2020, la política para el uso de la firma electrónica en los procesos jurisdiccionales y administrativos por parte de los jueces, juezas y demás servidores judiciales, para de esta manera lograr:

- Reducir el tiempo necesario para firmar una decisión. En particular todas las decisiones que involucren varios servidores judiciales.
- Aumentar la seguridad jurídica mediante la consulta y verificación de las decisiones contra el protocolo digital de decisiones u otros acervos digitales institucionales.
- Agilizar la emisión de las certificaciones de decisiones necesarias a terceros.
- Establecer el Protocolo de Decisiones Judiciales Digitales del Poder Judicial y otros repositorios de documentos de naturaleza administrativa, que serán mantenidos como consecuencia del cambio de paradigma resultado de este emprendimiento.

La Firma Electrónica podrá ser utilizada en todos los documentos producidos por los órganos jurisdiccionales y administrativos del Poder Judicial y sus dependencias, mediante el uso del Sello Electrónico Cualificado (Anexo 1, Título III, Resolución núm. 071-19, dictada por el Instituto Dominicano de las Telecomunicaciones) para concluir los procesos de firmas electrónicas.

Todos los documentos firmados electrónicamente por el poder Judicial serán solamente utilizados en formato PDF. En ese formato la verificación del documento se logrará mediante las funciones de firmas incluidas en el lector de PDF.

Cualquier usuario mediante el lector de PDF podrá verificar:

- El Sello Electrónico del Poder Judicial.
- La validez de la identidad del firmante.
- La ausencia de modificaciones en el documento posteriores al sellado.
- El origen de los elementos de confianza es de una de las autoridades competentes.

En caso de las copias en papel, la estampa final del documento arrojará información que facilitará verificar su fidelidad al original digital, siguiendo las instrucciones que estarán disponibles en el sitio web del Poder Judicial.

¿Qué hacer para tener una firma electrónica?

1



Solicitud: Solicitas el certificado junto con los requisitos indicados a una entidad que sea Prestadora de Servicios de Certificación. Ellos revisarán los requisitos entregados.



2



Acreditación: La Prestadora de Servicios de Certificación comprueba tu identidad, debes tener tu cédula contigo. Si representas una entidad o persona jurídica debes tener los documentos que así lo acrediten.

** Este proceso se puede realizar por videoconferencia realizando las pruebas de vida de la persona que solicita, ej.: mostrar el periódico del día junto a la cédula.*

3



Emisión: El Prestador de Servicios de Certificación crea con los dispositivos técnicos adecuados el par de claves pública y privada, y genera el Certificado de Firma Electrónica que garantiza tu identidad.

¿Cómo se usa una firma electrónica?

El firmante genera una "huella digital" del mensaje (mediante una función matemática). Esta huella digital se cifra con la clave privada del firmante, y el resultado es lo que se denomina firma electrónica la cual se enviará adjunta al mensaje original. El firmante agrega al documento una marca que es única y que solo él es capaz de producir, **¡su firma en el mundo digital!**

La jornada va a depender del tipo de herramienta que usemos para la firma, aquí te mostramos algunas:

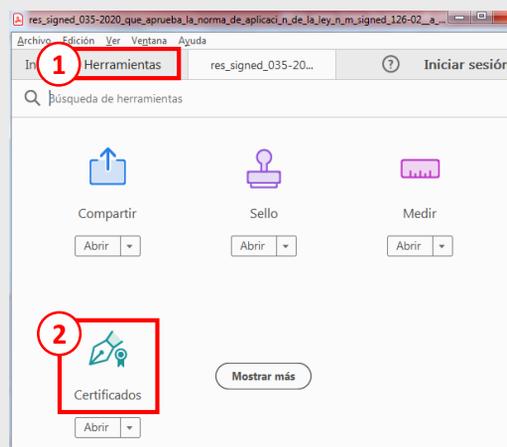
Desde un visor de PDF

Puedes usar tu certificado digital directamente en distintos visores de archivos PDF (no limitativo), como es el caso del Adobe Acrobat Reader DC (altamente recomendado).

1. Abres el documento a firmar en dicha aplicación y haces click en la opción **Tools (Herramientas)**, que se encuentra en el menú de la barra de opciones.
2. Dentro de este menú, haces click en la opción **Certificates (Certificados)**
3. Luego haces click en la opción **Digitally Sign (Firmar digitalmente)**, entonces haces

click y arrastras con el ratón o mouse para indicar el área donde deseas que aparezca la firma.

4. Una vez sueltas el ratón saldrá un recuadro donde debes elegir el certificado digital con que realizarás la firma y haces click en **Continue (Continuar)**.
5. Verás en pantalla tu sello visual de firma, y haces click en **Sign (Firmar)**.
6. Después de firmar, guardas el documento en la carpeta que desees, haciendo click en **Save (Guardar)**, te pedirá la clave o password del certificado, la colocas y haces click en **Allow (Permitir)**.



¿Cómo se usa una firma electrónica?

Desde un portafirmas

Solución que centraliza las operaciones de firma electrónica. Es muy similar a una bandeja de correo electrónico, donde se reciben los documentos a ser firmados, y se decide si firmar o rechazar el documento. Una vez firmado, se envía por email o se guarda el documento en el dispositivo (computadora o teléfono móvil).

Si tienes varios certificados digitales instalados, se podrá seleccionar con cuál se firmará cada documento. También permite la firma masiva, es decir, firmar varios documentos a la vez.

1. Entrás en la bandeja de firmas o inbox de la herramienta, y haces click en el mensaje que quieres firmar, el cual puede incluir archivos adjuntos o anexos.
2. Una vez revisas el contenido del mismo, haces click en el botón de **Firmar**.

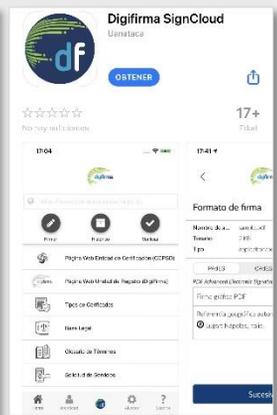
Firmas masivas: también puedes seleccionar varios elementos de la bandeja de entrada, y hacer click en Firmar, seleccionas el certificado digital y quedarán firmados los múltiples elementos seleccionados.



Aplicaciones móviles

Las Entidades de Certificación disponen de aplicaciones para realizar la firma electrónica desde los teléfonos móviles para mayor conveniencia:

- Avansi – Viafirma Inbox, Viafirma Documents, Viafirma Mobile, etc...
- Cámara de Comercio y Producción de Santo Domingo – Digifirma SignCloud

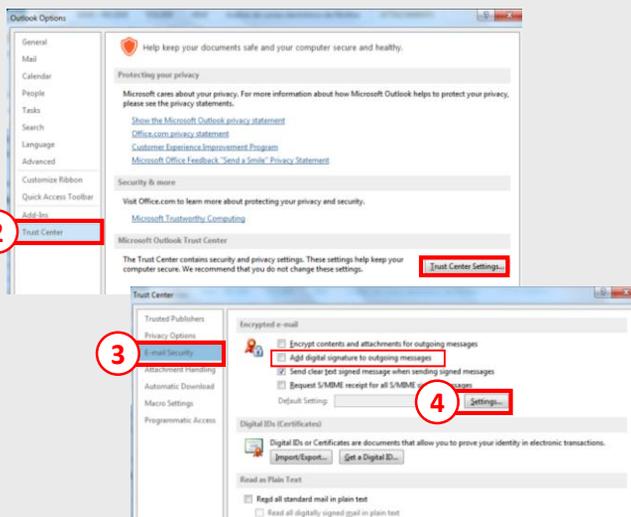


¿Cómo se usa una firma electrónica?

Desde un Correo Electrónico

Puedes configurar el certificado digital en un gestor de correo electrónico como Outlook, para firmar los mensajes que envías:

- 1- Seleccionas **File** en la barra superior del menú de opciones. Luego haces click en **Options** y aparecerá un recuadro de opciones.
- 2- Haces click en la parte inferior de la columna izquierda, **Trust Center** y eliges la opción de **Trust Center Settings**.
- 3- Eliges **E-mail Security** en la columna izquierda, y colocas un cotejo en la opción de **Add digital signature to outgoing messages**.

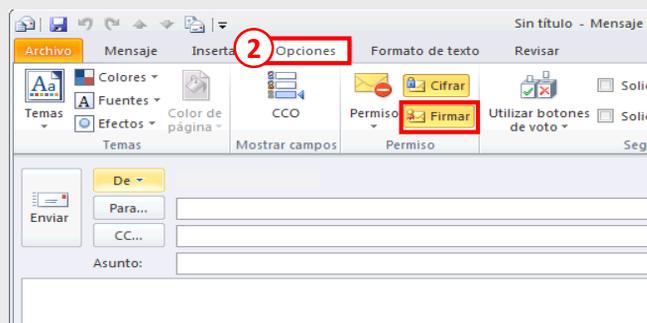


- 4- En **Settings** buscas el certificado digital que deseas instalar y haces click en **OK**, y al cerrarse ese recuadro haces nuevamente click en **OK**. **¡Ya está configurado!**

Para usarlo en tus mensajes de correo:

- 1- Creas un nuevo correo electrónico, redactas el mensaje, por ejemplo: una propuesta comercial.
- 2- Eliges **Options (Opciones)** en la barra superior del menú, y luego **Sign (Firmar)**.

Tu computadora agrega a ese mensaje electrónico una función hash (algoritmo), mediante la cual obtiene un resumen de ese mensaje (ocurre interno en la computadora). Tu computadora cifra ese mensaje-resumen utilizando tu clave privada.



Motor de firma

Es una solución en la que se puede realizar autenticación digital con certificados digitales de cualquier Prestador Cualificado de Servicios de Confianza.

Esta ofrece diferentes modalidades de firma electrónica:

- **firma centralizada** (con y sin intervención del usuario),
- **firma en cliente** (con intervención del usuario),
- **firma en lote** (varios documentos),
- **multifirma** (varios firmantes), firma de emails, etc.

Firma electrónica desatendida/ o en el servidor

Este tipo de firmas no requieren intervención del usuario y se realiza utilizando un certificado digital que puede residir en un almacén basado en software:

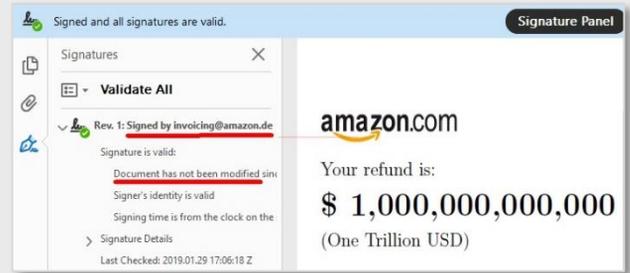
- Cacert de la JVM (Almacén de certificados de la Máquina virtual de Java).
- Pool de certificados (Repositorio centralizado) o bien, en un almacén basado en hardware:
- HSM (Módulo de Seguridad Hardware).

Procedimiento de verificación de firma electrónica

Es el proceso utilizado para determinar la validez de una firma electrónica. Dicho proceso debe constar por lo menos, de los pasos siguientes:

1. La verificación de que dicha firma electrónica ha sido creada durante el período de validez del **certificado digital** del suscriptor, en tiempo contra las fuentes de validación del certificado, para confirmar que no esté ni vencido ni revocado;
2. La comprobación de que dicha firma electrónica ha sido creada utilizando los datos de creación de firma electrónica correspondientes a los datos de verificación de firma electrónica indicados en el certificado del suscriptor; y,
3. La verificación de la autenticidad y la validez de los certificados involucrados.

4. La **firma electrónica** se valida al abrir el documento, momento en el cual saldrá un mensaje en el panel de firmas, que puede ser positivo indicando la validez de la misma con un símbolo verde, o negativo con un símbolo de alerta o unas aspas rojas.



Se puede elegir convertir el documento en formato *.PDF una vez firmado o dejarlo en el formato original. Habitualmente se firman PDFs, pero si se firma otro tipo de documento editable como un Word o un Excel y posterior a la firma alguien intenta modificarlo, saldrá un mensaje de alerta en dicho documento indicando que si el mismo fuera modificado las firmas perderán su validez.

¿Cómo se ve la firma electrónica?

La firma electrónica es un archivo digital, por lo que no se puede ver. Sí se puede diseñar para representarla gráficamente como un **"sello visual de firma"** o **"seguro de verificación"** para verificar la integridad del documento impreso en su versión original digital, que podría ser un código QR o de barras, como también puede ser cualquier otro tipo de imagen. En el caso de los códigos QR o código de barra, al ser escaneados nos redirigen a la plataforma de verificación donde se puede visualizar el documento original en formato digital.



"En un sector donde la inmediatez es importante, la inclusión de la firma y los certificados digitales han ayudado en el proceso de apertura de cuentas y otras operaciones, reduciendo significativamente los tiempos y evitando el desplazamiento de nuestros clientes."

Santiago De la Cruz | Alpha Inversiones



1. <https://www.indotel.gob.do/telecomunicaciones/firma-digital/>
2. <https://www.viafirma.do/>
3. <https://www.camarasantodomingo.do/digifirma/Home/Digifirma>
4. <https://optic.gob.do/firma-digital/>
5. <https://dgii.gov.do/cicloContribuyente/facturacion/comprobantesFiscalesElectronicos E-CF/Paginas/default.aspx>
6. https://www.poderjudicial.gob.do/documentos/PDF/doc_adjuntos_noticias/DAN_politica_de_firma_electronica_del_poder_judicial.pdf
7. La firma digital en el Departamento de Recursos Humanos, Docuten
8. eSignatures 101, Introducción a la Firma Electrónica. Signaturit
9. eBook: Todo lo que necesitas saber acerca de las firmas electrónicas, DocuSign
10. <https://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html>
11. Solución de firma biométrica para el sector financiero, BeSign de Serban Biometrics
<http://www.serbanbiometrics.es/es/soluciones/firma-digitalizada-biometrica>

Marcos regulatorios internacionales de servicios de confianza:

1. Reglamento de la Unión Europea núm. 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas (denominado eIDAS).
2. Foro de Autoridades de Certificación y Navegadores CA/B Fórum.
3. Sello de confianza Webtrust (American Institute of Certified Public Accountants (AICPA) y el Canadian Institute of Chartered Accountants (CICA)).
4. Programas propietarios de inclusión de confianza a certificados raíces como es el Approved Trust List de Adobe Reader.

Consideraciones de software

1. Se recomienda utilizar la versión de **ADOBE ACROBAT READER DC**. La misma es gratuita y la pueden encontrar en este enlace <https://get.adobe.com/es/reader/>
2. Se recomienda además tener Java Script en la computadora para el correcto funcionamiento de las distintas herramientas.

Agradecemos la colaboración de las siguientes entidades en la elaboración de este documento.





Asociación Dominicana de Empresas FinTech

Somos una **asociación sin fines de lucro** que **agrupa empresas FinTech** en la República Dominicana, cuyo objetivo es reunir a las empresas y/o expertos del área para que crezcan con sus **experiencias y conocimientos**, compartan y contribuyan con diferentes perspectivas, procurando **mejorar y aportar nuevas ideas** que reformulen la forma de entender y prestar servicios y **lograr mayor inclusión financiera**.

