firmadigital.bo

Firma Digital y Certificados Digitales

Una firma digital reconocida debe cumplir las siguientes propiedades o requisitos:

- Identificar al firmante.
- Verificar la integridad del documento firmado.
- Garantizar el no repudio en el origen.
- Contar con la participación de un tercero de confianza.
- Estar basada en un certificado digital reconocido.
- Debe de ser generada con un dispositivo seguro de creación de firma.

Los cuatro primeros puntos son posibles gracias al uso de las claves criptográficas contenidas en el certificado y a la existencia de una estructura de Autoridades de Certificación que ofrecen confianza en la entrega de los certificados; en Bolivia, esta estructura se denomina INCD: Infraestructura Nacional de Certificación Digital.

Para que la firma digital sea equivalente a la manuscrita, es decir, que una Firma digital sea reconocida, debe además:

"Estar basada en un Certificado Reconocido"

El certificado debe haber sido reconocido por la Autoridad de Fiscalización y Regulación de Telecomunicaciones y Transportes - ATT como autorizado para crear firmas reconocidas y debe estar listado en su página web.

Se pueden ver todos los certificados reconocidos por la ATT en la dirección:

https://att.gob.bo/content/firma-digital

firmadigital.bo

Son certificados reconocidos porque tanto la entidad que los emite como el contenido mismo del certificado, cumplen con los requisitos declarados en la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019 que aprueba los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras".

"Ser generada con un dispositivo seguro de creación de firma"

Las características de un dispositivo seguro de creación de firma están recogidas en el parágrafo II del Artículo N° 3 (INCORPORACIONES) del Decreto Supremo N° 3527 de fecha 11 de abril de 2018 que establece: "Se incorpora el inciso l) en el Parágrafo I del Artículo 27 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, aprobado por Decreto Supremo N° 1793, de 13 de noviembre de 2013, con el siguiente texto: 'l) Identificar su nivel de seguridad, en caso que el par de claves sea generado por dispositivo éste tendrá nivel de seguridad alto, en caso que el par de claves sea generado por software éste tendrá nivel de seguridad normal'".

Principalmente, el dispositivo seguro debe garantizar que las claves sean únicas y secretas, que la clave privada no se puede deducir de la pública y viceversa, que el firmante pueda proteger de forma fiable las claves, que no se altere el contenido del documento original y que el firmante pueda ver qué es lo que va a firmar.

ADSIB emite Certificados digitales en Bolivia

La ADSIB es la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, entidad pública de servicios tecnológicos, designada como única Entidad Certificadora Autorizada Pública encargada de emitir Certificados para Firma Digital

Toda la validez legal que necesitas

A partir de la Ley 164: Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, del 08 de agosto de 2011, la Firma Digital tiene validez jurídica y probatoria.

firmadigital.bo

No te confundas

La firma digital se realiza a través de un CERTIFICADO DIGITAL emitido por una entidad certificadora autorizada.

Un CERTIFICADO DIGITAL es un conjunto de elementos digitales que identifican a una persona en el mundo digital.

ADSIB es la única Entidad Certificador Autorizada Pública en el PAÍS con trámite 100% en línea y con todas las medidas de seguridad necesarias para garantizar un óptimo procedimiento.

Tipos de los Certificados Digitales

Los tipos de perfiles de Certificados Digitales que podrán emitir las Entidades Certificadoras Autorizadas, conforme a estándares internacionales, son los siguientes:

- **Certificado de Persona Natural:** Documento digital que pertenece y contiene los datos de una persona (nombre, número de CI y correo electrónico).
- **Certificado de Persona Jurídica:** Documento digital que pertenece y contiene los datos de una persona que figura en representación de una entidad pública o privada (nombre, número de CI, correo electrónico, cargo y nombre de la institución).

firmadigital.bo

El formato para los tipos de Certificados Digitales está basado en el RFC 5280 y están definidos en el Anexo 1 del documento "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados según Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019.

Nivel de seguridad de los Certificados

Desde un punto de vista técnico, según el Artículo N° 6 del documento "Estándar Técnico para la Emisión de Certificados Digitales", aprobado mediante Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019, se establecen dos alternativas para el resguardo de las claves según su nivel de seguridad:

- **NIVEL DE SEGURIDAD NORMAL: Certificados Digitales emitidos por dispositivo criptográfico basado en Software.** El solicitante deberá generar el par de claves (público y privada) por software, en un dispositivo seguro que cumpla con el estándar FIPS 140-2 nivel 1 mínimamente, posteriormente debe proporcionar a la Entidad Certificadora Pública ADSIB la solicitud de firma de Certificado – CSR en un archivo electrónico que contiene el requerimiento de firma de certificado. El certificado digital, así como su par de claves, serán resguardados por el usuario titular en un contenedor PKCS#12 (archivo con la extensión .p12) .
- **NIVEL DE SEGURIDAD ALTO: Certificados Digitales emitidos por dispositivo criptográfico basado en hardware.** El solicitante deberá generar el par de claves (pública y privada) en un dispositivo que cumpla con el estándar FIPS 140-2 nivel 2 mínimamente, posteriormente debe proporcionar a la Entidad Certificadora Pública la solicitud de firma de Certificado – CSR en un archivo electrónico que contiene el requerimiento de firma de certificado.

firmadigital.bo

Dependiendo del tipo del nivel de seguridad que se vaya a utilizar, se deberá contar con lo siguiente:

- **Nivel de seguridad NORMAL:** Archivo p12 donde sea almacenado el Certificado digital que permita firmar uno o varios documentos y que cumpla con sistemas de seguridad reconocidos internacionalmente garantizando la confiabilidad del mismo (inciso g) art. 33 del D.S. 1793).
- **Nivel de seguridad ALTO:** Dispositivo que permita firmar un documento al signatario, donde sean almacenados y custodiados el Certificado Digital y su clave privada (Token o tarjetas inteligentes – Smart cards) que cumpla con el estándar FIPS 140-2 (inciso g) art. 33 del D.S. 1793 y sus modificaciones descritas en el D.S. 3527), homologado por la ATT.

Los certificados digitales emitidos a través de dispositivos criptográficos basados en software solo podrán ser utilizados por Personas Jurídicas, siempre y cuando sean administrados en condiciones técnicamente seguras y confiables, que eviten su uso por terceros no autorizados.

Forma de uso de la Firma

La forma de uso del Certificado Digital está definida por cómo el usuario titular firma los documentos:

- **Firma Digital Automática:** Firma digital generada por un sistema informático, donde el titular del certificado digital delega su uso para tareas definidas en éste.
- **Firma Digital Simple:** Firma digital generada con intervención DIRECTA del usuario titular (normalmente representada por el ingreso del PIN en cada proceso de firmado).

Los certificados digitales con seguridad Alta o Normal podrán ser usados para realizar Firma Digital Automática, siempre y cuando el firmado se realice en condiciones técnicamente seguras y confiables, que eviten su uso por terceros no autorizados.

Para la realización de la firma digital de forma automática, se debe comprobar que los datos con los que se creare sean controlados por medios que permitan evitar de forma técnicamente segura y confiable su uso por terceros no autorizados, para otros fines que no se encuentren descritos en el certificado digital.

Solicitar un Certificado Digital

Durante el proceso de solicitud de un Certificado Digital, la Entidad Certificadora debe acreditar la identidad del titular del Certificado, por lo que la solicitud es personal y de manera presencial, para confirmar su inequívoca identificación.

Además, cada usuario solicitante deberá definir previamente los aspectos relacionados a su Certificado Digital en base a sus necesidades y en el marco de los aspectos mencionados en este documento:

- **Perfil del Certificado Digital:** Persona natural / Persona Jurídica.
- **Nivel de Seguridad:** Alto / Normal
- **Medio de almacenamiento:** Software / Token o HSM
- **Forma de uso:** Firma Simple / Firma Automática

Además, ten listo los requisitos según el perfil del Certificado que vayas a solicitar:

- Certificado de Tipo Persona Natural
  - Carnet de identidad nacional o extranjero
  - Factura de pago de luz, agua o teléfono
- Certificado de Tipo Persona Jurídica
  - Carnet de identidad nacional o extranjero
  - Autorización original de la persona jurídica firmada por el Representante Legal o MAE
  - Documento de Exhibición del NIT.

Una vez tengas todo listo y definido, puedes realizar el procedimiento de solicitud totalmente en línea a través de: https://solicitud.firmadigital.bo/

- ✓ Ingresa a solicitud.firmadigital.bo
- ✓ Darse de alta como usuario en el botón "Registrate"
- ✓ Ingresar y crear una nueva solicitud
- ✓ Elegir Perfil de Certificado
- ✓ Carga los requisitos según el Perfil de Certificado
- ✓ Sube tu selfie
- ✓ Paga por el servicio en línea

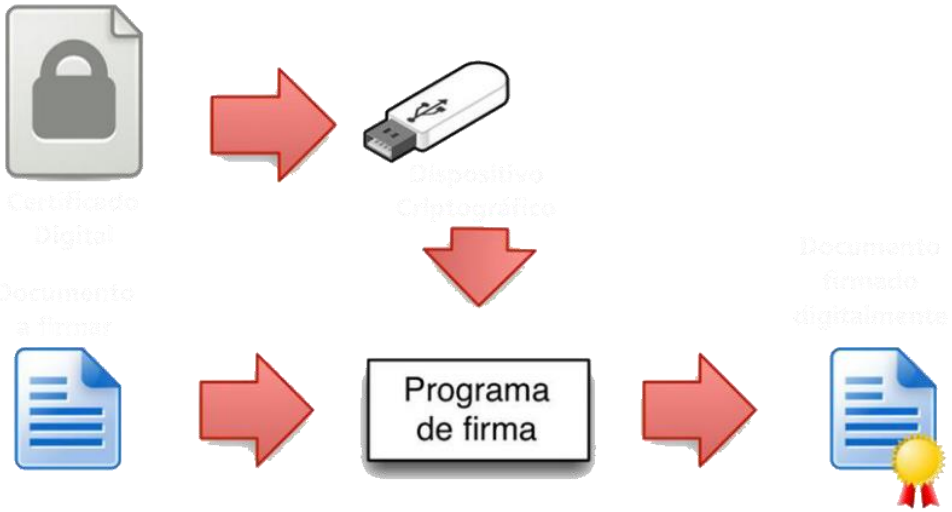
firmadigital.bo

Puedes ver cómo se realiza el proceso de solicitud a través de nuestros videos que indican el procedimiento paso a paso:

Guía para solicitar tu Certificado digital

¿Cómo se firma con un Certificado Digital?

Para Firmar digitalmente con tu Certificado, necesita el documento, tu Certificado Digital y una aplicación compatible con el uso de Certificados Digitales



Puedes ver nuestros ejemplos de uso de Firma Digital:

- Firma Digitalmente documentos PDF con Jacobitus FIDO
- Firma Digitalmente documentos PDF con Jacobitus SOFT y usando certificados P12
- Firma Digitalmente documentos PDF con Acrobat Reader
- Firma Digitalmente documentos PDF con Acrobat Reader y usando certificados P12
- Firma Digitalmente tus correos con Mozilla Thunderbird
- Firma Digitalmente tus correos con Ms Outlook
- Firma Digitalmente documentos en Ms Word

firmadigital.bo