Ciudad de México a 11 de Marzo del 2010.

A quien corresponda

El certificado digital, es una identificación oficial electrónica, emitida por una entidad autorizada, como lo es una Autoridad Certificadora.

A través de este certificado el cual cuenta con dos llaves (privada y pública) podrá firmar de manera electrónica cualquier tipo de documento.

La Firma Electrónica Certificada es un conjunto de datos que se adjuntan a un mensaje electrónico, **cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa.**

Por sus características, la Firma electrónica certificada **brinda seguridad a las transacciones electrónicas,** con su uso se puede identificar al autor del mensaje y verificar no haya sido modificado.

Su diseño se basa en estándares internacionales de infraestructura de claves públicas (o PKI por sus siglas en inglés: Public Key Infrastructure) en donde se utilizan dos claves o llaves para el envío de mensajes:

La "llave o clave privada" que únicamente es conocida por el titular de la Firma Electrónica, que sirve para cifrar datos; y

La "llave o clave pública", disponible en Internet para consulta de todos los usuarios de servicios electrónicos, con la que se descifran datos. En términos computacionales es imposible descifrar un mensaje utilizando una llave que no corresponda.

El uso de la Firma Electrónica en México

Secretaría de Economía.

DECRETO por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de Firma Electrónica.

Artículo 89 bis.

No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Artículo 90.

Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:

I. Por el propio Emisor;

II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o

III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.

Artículo 90 bis.

Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por lo tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia, cuando:

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o

II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía, resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio.

Es así que la responsabilidad del uso y conocimiento de la contraseña del certificado, es del titular del mismo, ya que hay que recordar que el electrónico es el equivalente al manuscrito y por ello la importancia de tramitarlo de manera personal y que nadie más que el solicitante, conozca dicha contraseña.

Atte.
Rebeca Flores Abedoy
Director Comercial
PSC Advantage