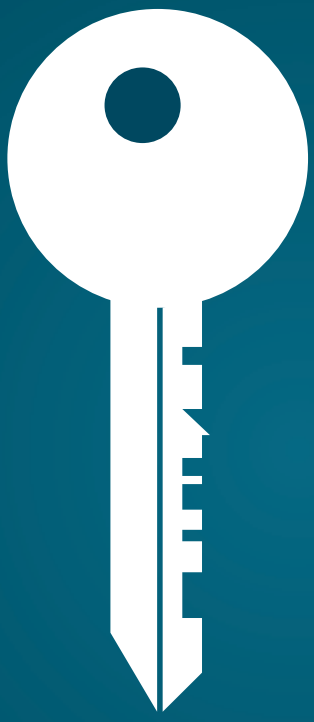


DOCUMENTO EXPLICATIVO DEL

ANTEPROYECTO DE LEY DE FIRMA ELECTRÓNICA

EL SALVADOR

Documento Explicativo del Anteproyecto de Ley de Firma Electrónica

Secretaría para Asuntos Legislativos y Jurídicos de la Presidencia
Ministerio de Economía
Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador

Presidencia de la República de El Salvador
Alameda Dr. Manuel Enrique Araujo, 5500 Casa Presidencial San Salvador, El Salvador, 2012

Juan Francisco González
Director de Innovación Tecnológica e Informática
del Gobierno de El Salvador

Erick Chang
Gerente de Investigación Estratégica

Iris Palma
Organización de Estados Americanos (OEA)

Diseño y diagramación
Área de Diseño y Conceptualización de la Gerencia de Investigación Estratégica.
Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador

Contenido

Presentación

La Ley de Firma Electrónica de El Salvador nace con el objetivo de reconocer el derecho a la seguridad jurídica de toda persona tomando en cuenta a la tecnología como el hilo que enlaza diversas dinámicas sectoriales de la sociedad; y, además, siendo ésta una deuda a la sociedad cuyas actividades están plenamente basadas en la tecnología, especialmente al interior del gobierno; pero también es una herramienta de confianza y facilidad para el desarrollo de sectores potenciales de la economía, y de su relación con el gobierno.

De esta pauta, la Firma Electrónica no viene sino a acompañar los esfuerzos de modernización e innovación actuales, y que encaminan a la sociedad en general hacia una transición sana e inclusiva a la sociedad del conocimiento.

Generar instrumentos legales como esta Ley es la confirmación de que las tecnologías son parte importante y estratégica de nuestra sociedad, y de que propiciar su legislación permitirá ofrecer a la sociedad un marco transparente y claro del clima de negocios, del fomento productivo y de las relaciones sociales.

Con este documento pretendemos exponer las generalidades del Anteproyecto de Ley de la Firma Electrónica (que ha sido incorporado al final como referencia), y presentar además una breve reseña del entorno internacional en la creación de la Ley de Firma Electrónica, y que han traído a diversos países beneficios que se vuelven en ahorros de tiempo y en costos de operación tanto para el sector empresarial como para el gobierno mismo.

Esperamos que el planteamiento expuesto en este documento le permita al lector contar con el escenario claro y amplio sobre la utilización de la Firma Electrónica y de las acciones que se verán reguladas con la implementación de esta Ley.

La Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador, y los aliados gubernamentales como la Secretaria Técnica, el Ministerio de Economía, entre otros, anhelamos que nuestros esfuerzos impacten en la consecución de una agenda de desarrollo, donde las tecnologías de la información y comunicaciones son por mucho el motor de la innovación y las responsables de cambios positivos y significativos en la productividad empresarial y en la administración pública.

Cordialmente,

Juan Francisco González
Director de Innovación Tecnológica e Informática
del Gobierno de El Salvador (ITIGES)

Glosario de términos

Acreditación: Es la autorización que otorga la Superintendencia General de Electricidad y Telecomunicaciones, SIGET, a los proveedores de servicios de certificación para operar y proporcionar certificados electrónicos y a los proveedores de servicios de almacenamiento de documentos electrónicos, una vez cumplidos los requisitos y condiciones establecidos en la presente Ley;

Certificado Electrónico: Documento proporcionado por un proveedor de servicios de certificación que otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con dicha firma;

Comunicación Electrónica: Toda información o mensajes de datos generado, enviado, recibido, archivado o comunicado por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos, EDI, el correo electrónico y otros;

Destinatario: La persona designada por el emisor para recibir el mensaje de datos, pero que no esté actuando a título de Intermediario con respecto a dicho mensaje;

Documento Electrónico: Todo mensaje de datos enviado, recibido o archivado por medios electrónicos, ópticos o de cualquier otra tecnología que forman parte de un expediente electrónico;

Firma: Comprenderá la firma electrónica simple y la firma electrónica certificada;

Firma Electrónica Simple: Son los datos en forma electrónica consignados en un mensaje de datos o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;

Firma Electrónica Certificada: Son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos;

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona que representa;

Iniciador de un Mensaje de Datos: Se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;

Proveedor de Servicios de Certificación: Persona jurídica autorizada por la SIGET, dedicada a emitir certificados electrónicos y demás actividades previstas en esta Ley;

Proveedor de Servicios de Almacenamiento Tecnológico de Documentos Electrónicos: Persona jurídica autorizada por la SIGET que, por la naturaleza de su negocio, brinda servicios de almacenamiento tecnológico de documentos electrónicos;

Signatario: Persona que posee un dispositivo de creación de firma y que actúa en nombre propio o a nombre de una persona natural o jurídica que representa;

SIGET: Superintendencia General de Electricidad y Telecomunicaciones.

Capítulo I

Fundamentos de Firma Electrónica

Introducción

El Anteproyecto de Ley de Firma Electrónica antecede al documento final de la Ley una vez esté suscrito en la Asamblea Legislativa. Para efectos de este documento todo a lo que se haga mención del Anteproyecto se entenderá es consecuente con la Ley en sí. Así, lo en concordancia con lo que se establece en el Anteproyecto de Ley de la Firma Electrónica de El Salvador, el concepto básico de la Firma Electrónica es aquella que al hacer uso de medios electrónicos no pierde la esencia de la firma manuscrita: identifica plenamente a una persona y cumple con la función de vincularse u obligarse con el contenido de un documento o mensaje firmado. En general, la Firma Electrónica es un método que asocia la identidad de una persona, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. En ese sentido, vale aclarar que la firma electrónica no se trata de una firma personal digitalizada o escaneada; tampoco se refiere a un password, ni a una huella digital y no se limita únicamente a una autenticación.

Más bien consiste en el uso de una gama de conceptos matemáticos por medio de los cuales se puede incluir en los documentos electrónicos un conjunto de datos en forma de claves que garantizan la efectividad de la transacción y brindan seguridad a las partes involucradas.

La importancia de fomentar la Ley de Firma Electrónica radica en la rápida, creciente y efectiva utilización de la tecnología para las relaciones entre los diversos actores de la sociedad, tanto a nivel local como internacional, que incluye, entre otros, un alto componente de negocios y gestiones

gubernamentales. Más allá de la reducción de tiempos en la comunicación, la Firma Electrónica tiene la virtud de ser un mecanismo de transparencia proporcionando el máximo grado de confidencialidad y seguridad en internet.

Esto último es indispensable en el camino estratégico de fomentar un clima de negocios ágil y seguro para las inversiones locales e internacionales, para incrementar la educación digital de la sociedad, para impulsar la modernización del Estado y dar continuación a lo establecido en la Ley de Acceso a la Información Pública, "Promover el uso de las tecnologías de la información y comunicación y la implementación del gobierno electrónico" Art. 3, literal g.

Un gobierno electrónico eficiente, eficaz y útil recae en una normativa, tal como la de la Firma Electrónica, que enmarque la administración electrónica en el gobierno como también en las relaciones sociales.

En las dinámicas empresariales, sociales y gubernamentales de la economía salvadoreña, el uso intensivo de internet ha implicado un nuevo estrato en la evolución de la comunicación.

En las diversas dimensiones de la oferta y la demanda de información, el papel del gobierno en el fomento de la incorporación de la tecnología (internet, maquinaria, software) en el sector empresarial ha resultado en una expansión positiva de nuevos negocios y la identificación de nuevos nichos y mercados de negocios; con esta lógica, una legislación de Firma Electrónica no vendría sino a acompañar los esfuerzos sociales a favor de la innovación para el bien común.

Vale mencionar que para efectos de definición, se refiere a la firma electrónica como un término de naturaleza legal y más amplia desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos; mientras que firma digital hace referencia a una serie de métodos criptográficos.

En general, la firma digital (en su aplicabilidad legal, firma electrónica) constituye una herramienta esencial para garantizar la debida seguridad y brindar confiabilidad a las transacciones, facilitando y proporcionando autenticidad entre partes que por diversas razones no ha podido, pueden o podrán encontrarse presencialmente.

En ese sentido, la Firma Electrónica es un elemento imprescindible para el desarrollo del comercio electrónico, la modernización de la administración pública, la generación de empleo, la agilidad de los trámites, la transparencia, y la gestión de negocios.

En consecutiva, a sumar a otras áreas estratégicas para el desarrollo.

Enmarcado en este contexto, el Anteproyecto de Ley de Firma Electrónica que acompaña este documento, está basado en la consideración que "el desarrollo de las tecnologías de información y comunicaciones se ha convertido en un factor estratégico que mejora la eficiencia de la educación, fomenta la competitividad y el crecimiento económico de los pueblos, asimismo eleva la calidad de vida de los ciudadanos, al permitir la inclusión de más personas al sistema productivo, razón por la cual nuestro país, por medio de la presente ley pretende promocionar el uso de estas tecnologías para propiciar el comercio y el desarrollo económico, incorporando al país al entorno mundial en que se producen interacciones seguras, dentro de la sociedad de la información".

Este postulado reconoce a la Firma Electrónica como un elemento más del complejo sistema de dinamismo económico y social del país, el cual se engrana por medio de un marco normativo y legal (e institucional) que da vida a las actuaciones de los actores sociales, procurando paralelamente una transición a la sociedad de la información.

Retomando lo expuesto en el documento, se plasman los objetivos finales del Anteproyecto:

- Equiparar la firma electrónica simple y firma electrónica certificada con la firma autógrafa;
- Otorgar y reconocer eficacia y valor jurídico a la firma electrónica certificada, a los mensajes de datos y a toda información en formato electrónico que se encuentren suscritos con una firma electrónica certificada, independientemente de su soporte material.
- Regular y fiscalizar lo relativo a los proveedores de servicios de certificación electrónica, certificados electrónicos y proveedores de servicios de almacenamiento de documentos electrónicos.

Sobre la Firma Electrónica

Firma digital: es un conjunto de métodos criptográficos y técnicos. Es un concepto fundamentalmente técnico.

Firma electrónica: es un término mucho más amplio y hace referencia a cuestiones legales, organizativas, técnicas, etc.

En general, la firma digital (en su aplicabilidad legal, firma electrónica) constituye una herramienta esencial para garantizar la debida seguridad y brindar confiabilidad a las transacciones, facilitando y proporcionando autenticidad entre partes que por diversas razones no ha podido, pueden o podrán encontrarse presencialmente.

En el Anteproyecto de Ley de Firma Electrónica de El Salvador, el concepto básico de la Firma Electrónica es, aquella que al hacer uso de medios electrónicos no pierde la esencia de la firma manuscrita: identifica plenamente a una persona y cumple con la función de vincularse u obligarse con el contenido de un documento o mensaje firmado.

En general, la Firma Electrónica es un método que asocia la identidad de una persona, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. En otras palabras un documento redactado en un procedador de textos (ya sea este MS Office, OpenOffice, Lotus, PDF, entre otros) u otros documentos electrónicos (Imagen, correo electrónico, un documento escaneado) firmado con “Firma Electrónica Certificada“, es equivalente a un documento impreso con firma manuscrita.

En ese sentido, vale aclarar que la firma electrónica no se trata de una firma personal digitalizada o escaneada; tampoco se refiere a una contraseña, ni a una huella digital y no se limita únicamente a una autenticación.

CARACTERÍSTICAS DE LA FIRMA ELECTRÓNICA:

- Sirve para identificar de forma inequívoca quien es el autor del documento.
- Es el signo principal que representa la voluntad del firmante de obligarse al compromiso pactado.
- Permite identificar si el autor de la firma es efectivamente aquel que ha sido identificado como tal en el acto de la propia firma.
- No puede ser generada más que por el emisor del documento, a excepción de aquellos casos donde la Ley permite que la firma electrónica de una persona jurídica o natural esté a la custodia de otra persona, y así sea expresado en el certificado digital.
- Las informaciones que se generen a partir de la firma electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.
- Permite transacciones en tiempo real y sin necesidad de la presencia de las partes.
- Facilita la automatización de procesos y reduce costos y tiempos de tramitación.

IMPORTANCIA DE LA FIRMA ELECTRÓNICA

La Legislación en Firma Electrónica es un reconocimiento al Artículo 2 de la Constitución de la República, el cual establece “el derecho a la seguridad jurídica de toda persona, por lo que el Estado debe crear un marco legal que brinde seguridad a los usuarios de las comunicaciones electrónicas, y a las transacciones autorizadas mediante las aplicaciones de la tecnología o la suscripción electrónica de las mismas brindándole validez jurídica”.

Lo anterior se enmarca perfectamente en el acontecer actual donde la tecnología y las comunicaciones por medios electrónicos y digitales tienen un papel protagónico dentro de las relaciones económicas, sociales, políticas y culturales de la sociedad. De acuerdo a Internet World Stats para septiembre del 2012, cerca de un millón y medio de personas en El Salvador son usuarios de Internet.

En el quehacer de las dinámicas sociales, el vínculo que genera la riqueza social radica en la facilidad, agilidad y confianza en el incremento oportuno de información, que en su máxima expresión genera conocimiento que en un fin último es uno de los factores claves de la innovación. Los flujos de información se han agilizado gracias a la apropiación de la tecnología como medio de difusión, y son precisamente estos cambios evolutivos los que se dan cuenta en gran medida de la dinámica relación entre el gobierno-sociedad y viceversa. Asimismo, vale resaltar las oportunidades derivadas del comercio exterior y el potencial del sector servicios de El Salvador que imprimen mayor relevancia al potencial de las tecnologías como medio para proveer y garantizar herramientas efectivas para el desarrollo.

Por otro lado, la Ley de Firma Electrónica recoge el espíritu de constituirse en un instrumento que acompañe a los esfuerzos gubernamentales que se han venido realizando en los últimos años para modernizar la administración pública, centrando al ciudadano como el eje de los servicios y trámites disponibles e internet.

En resumen, la Firma Electrónica tiene implicaciones positivas al interior de la gestión pública, y al mismo tiempo el alcance de su beneficio es replicable en el impulso del comercio electrónico del país. Además de servir como base para el desarrollo de otras iniciativas de la e-administración como lo son la factura electrónica, trámites en línea, entre otros.

COMPONENTES DE LA FIRMA ELECTRÓNICA

Para utilizar la Firma Electrónica es necesario hablar primero de cinco componentes que sistemáticamente resultan en una firma digital propiamente aplicada.

» PRIMERO: DOCUMENTOS ELECTRÓNICOS

Un documento electrónico es un documento cuyo soporte es electrónico o magnético; su contenido es codificado digitalmente. Algunos de estos documentos se refieren a correos electrónicos, datos ingresados a un formulario, una transacción bancaria, una imagen (scan) de un documento en papel, un archivo cualquiera de la PC, una grabación de audio o video, un contenido de un CD, entre otros.

» SEGUNDO: INTEGRIDAD DE LOS MENSAJES DIGITALES

Una de las características de la firma electrónica es la “integridad” de los mensajes electrónicos, que tiene como objetivo garantizar la inalterabilidad de los documentos ya firmados con la firma electrónica certificada; esto es posible gracias a la función hash que es una algorítmo que resume un gran conjunto de datos, dando como resultado otro conjunto de datos finito. En otras palabras, selecciona datos de un mensaje digital por medio de un conjunto de códigos.

La Función Hash son funciones matemáticas que realizan un resumen del documento. El mecanismo es comprimir el documento electrónico en un único bloque de longitud física, es decir que el resumen es representado por un número fijo.

Su mecanismo:

- El emisor del documento aplica una Función Hash lo cual obtiene un número finito que es el resumen del documento.
- Dicho resumen se encripta en una llave privada de la firma electrónica certificada.
- El emisor envía al receptor el documento electrónico encriptado.
- El receptor aplica la Función Hash al resumen sin encriptar y desencripta

Por ejemplo el código ASCII asigna a cada carácter un número tanto para mayúsculas como minúsculas y símbolos especiales, como se presenta en el cuadro:

65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
,	.	–	;	:	–	[	]	{	}	´´	+	*	¿	?

Cuando se escribe un mensaje electrónico, cada carácter es representado por un código según la codificación ASCII, incluyendo los espacios:

69	108	32	108	111	98	111	32	98	108	97	99	111	32	
E	l		l	o	b	o		b	l	a	c	o		
99	97	109	105	110	97	32	101	110	32	108	97	32		
c	a	m	i	n	a		e	n		l	a			
99	111	108	105	110	97	32	108	101	106	97	110	97	32	
c	o	l	i	n	a		l	e	j	a	n	a		

Para determinar la integridad de un mensaje electrónico, si usamos el método ASCII, la función hash hará una operación lógica por cada 3 caracteres de la siguiente manera: (1° carácter – 2 carácter)*3° carácter, luego se suman los resultados generando un número específico.

Si al mensaje electrónico se le hace cualquier cambio, por mínimo que este sea, como colocarle un signo de puntuación, una mayúscula, etc.

El número asignado al mensaje electrónico cambiará:

69	108	32	108	111	98	111	32	98	108	97	99	111	32	
E	l		l	o	b	o		b	l	a	c	o		
	–1248			–294			7742			1089			7821	15110
99	97	109	105	110	97	32	101	110	32	108	97	32		
c	a	m	i	n	a		e	n		l	a			
		–1260			416			–288			352			–780
99	111	108	105	110	97	32	108	101	106	97	110	97	32	
c	o	l	i	n	a		l	e	j	a	n	a		
	–1296			–485			–7676			990			60	–8407

5923

Como se puede ver en el ejemplo anterior, a pesar que los dos mensajes signifiquen los mismo no son idénticos ya que el segundo presenta una diferencia en haberle colocado una mayúscula; aunque sea la misma letra, cuando es mayúscula o minúscula su codificación ASCII cambia, por lo tanto al realizar un cambio, el número resumen es diferente en los dos mensajes.

Mensaje 1

69	108	32	108	111	98	111	32	98	108	97	99	111	32	
E	l		l	o	b	o		b	l	a	c	o		
	–1248			–294			7742			1089			7821	15110
99	97	109	105	110	97	32	101	110	32	108	97	32		
c	a	m	i	n	a		e	n		l	a			
		–1260			416			–288			352			–780
99	111	108	105	110	97	32	108	101	106	97	110	97	32	
c	o	l	i	n	a		l	e	j	a	n	a		
	–1296			–485			–7676			990			60	–8407

Mensaje 2: Es el primer mensaje solamente que se cambió una letra de minúscula y mayúscula.

69	108	32	108	111	98	111	32	66	108	97	99	111	32	
E	l		l	o	b	o		B	l	a	c	o		
	−1248			−294			5214			1089		7821		12582
99	97	109	105	110	97	32	101	110	32	108	97	32		
c	a	m	i	n	a		e	n		l	a			
	−1260			416			−288			352				−780
99	111	108	105	110	97	32	108	101	106	97	110	97	32	
c	o	l	i	n	a		l	e	j	a	n	a		
	−1296			−485			−7676			990		60		−8407
														3395

Mensaje 1: 5923 No es igual a Mensaje 2: 3395

Un ejemplo práctico de la función Hash

Caso 1

Nicolás tiene una empresa de servicios y redacta un contrato con Alejandra para realizar ciertas tareas de manera siguiente:

“Como representante de ‘Empresas Verdes’ se compromete con la ‘Empresa A’ a realizar las siguientes tareas:

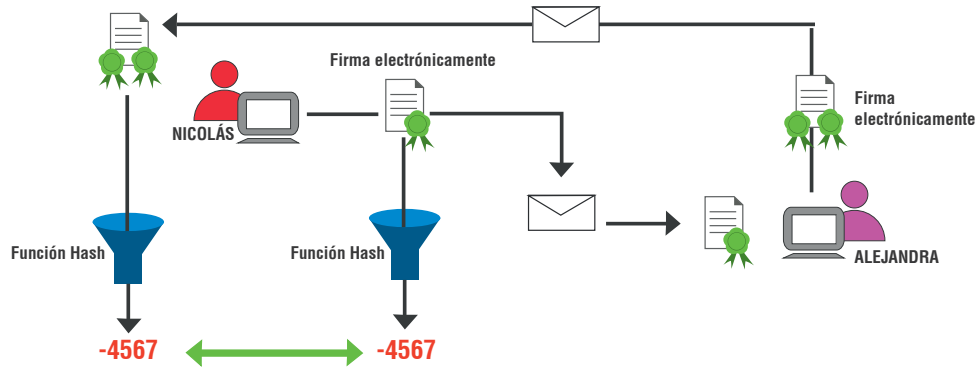
- Análisis de impacto ambiental de los procesos de la Empresa A
- Generación de 3 informes de investigación sobre cada uno de los 10 proceos
- Dichos informes serán entregados a 2 meses después de firmado el contrato.
- Trás aprobación de la Empresa A, se realizará un pago de $10,000 al finalizar dichas tareas

La persona que recibirá y dará el visto bueno será la representante de la Empresa A, la señorita Alejandra.

Atentamente

Nicolás”

Nicolás al redactar el documento, lo firma electrónicamente y al hacer eso, una de las características de la firma electrónica certificada es que al documento le realiza un cálculo mediante la función hash cuyo resultado en este caso -4567. Nicolás le envía por correo electrónico el documento a Alejandra para su aprobación y posterior firma. Alejandra al leer el contrato y al estar de acuerdo lo firma con firma electrónica certificada y es enviado a Nicolás, quien al recibirlo, comprueba su integridad al hacer nuevamente el cálculo mediante la función hash y le da como resultado -4567, eso quiere decir que el documento no ha sido alterado por Alejandra.



Caso 2

Nicolás también tiene un cliente que es la Empresa B quien es representado por Rogelio, en este caso la Empresas Verdes ha realizado ya una serie de tareas y están en el procedimiento del pago respectivo. Nicolás manda un documento donde detalla:

“Como representante de ‘Empresas Verdes’ dando el cumplimiento a las tareas realizadas a la ‘Empresa B’ representado por Rogelio se realizaron las siguientes tareas:

- Análisis de impacto ambiental de los procesos de la Empresa B entregado el día 3 de febrero. Con un costo de $3,000
- Generación de 3 informes de investigación sobre cada uno de los 5 procesos entregado el día 10 de marzo. Con un costo de $4,000
- Con un total de $7,000

Atentamente

Nicolás"

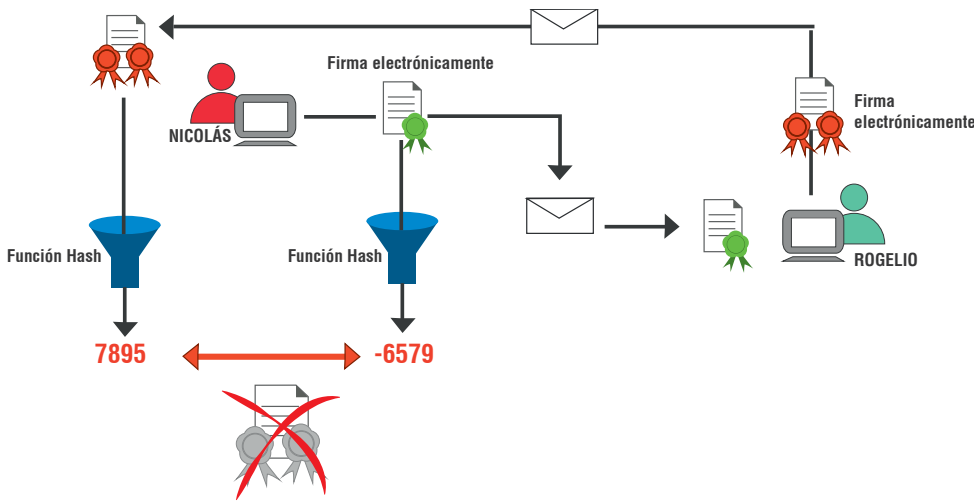
Dicho documento es firmado por Nicolás y el resultado del cálculo lógico de la función hash es de 7895; este documento es enviado a Rogelio. Antes que Rogelio lo haya firmado realiza unos cambios al documento.

"Como representante de 'Empresas Verdes' dando el cumplimiento a las tareas realizadas a la 'Empresa B' representado por Rogelio lo cual se realizaron las siguientes tareas:

- Análisis de impacto ambiental de los procesos de la Empresa B entregado el día **7 de febrero**. Con un costo de $3,000
- Generación de 3 informes de investigación sobre cada uno de los 5 procesos entregado el día 10 de marzo. Con un costo de $4,000
- Con un total de $7,000

Atentamente

Nicolás"



Rogelio le envía el documento firmado electrónicamente a Nicolás. Al recibirlo Nicolás, comprueba la integridad del documento y después del cálculo lógico de la función Hash dio como resultado: -6579, comprobando que el documento ha sido alterado, por lo cual dicho documento queda totalmente invalidado.

En el caso concreto de la firma electrónica certificada, el mecanismo por el cual aplica dicha función no es ASCII, sino que utiliza otras cuyo codificación no es pública, por ejemplo: MD2, MD4, MD5, SHA-1, RIPEND-160.

» TERCER: LLAVE PRIVADA

La llave privada (o clave privada) es una cadena de longitud variable de dígitos que conforman una serie numérica y se obtiene a partir de la aplicación de algoritmos matemáticos complejos donde la probabilidad de tener dos claves privadas iguales es casi cero. La llave privada se obtiene a partir de una función matemática que es el complemento aritmético perfecto de la llave pública asociada pero siendo no derivable, es decir, es imposible llegar a la otra conociendo una de estas.

La llave privada cifra el documento electrónico. El resultado es la firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir.

La llave privada es exclusiva del firmante, y puede ser guardada en dispositivos electrónicos como chips, memorias usb, archivos.

» CUARTO: LLAVE PÚBLICA

La llave pública es de uso general y son los Proveedores de Certificados que tienen la obligación de suministrarla y publicarla en sus sitios Web para efectos de verificación de la identidad de quien posea un certificado digital o para verificar la integridad de un documento firmado digitalmente.

Esta llave hace parte del sistema de "Infraestructura de Clave Pública" (PKI por sus siglas en inglés) y representa uno de los puntos de partida más importantes para la seguridad de la información. La llave pública es una cadena de longitud variable de dígitos que conforman una serie numérica y se obtienen a partir de la aplicación de algoritmos matemáticos complejos y de esta forma garantizan que la probabilidad de encontrarse

dos claves públicas iguales sea casi cero. La llave pública se obtiene a partir de una función matemática que es el complemento perfecto de la llave privada asociada siendo estas no derivables. Es decir, conociendo una de estas es imposible llegar a la otra. Por ejemplo, Daniel quien tiene una empresa que brinda un servicio y cuyos contratos lo hace de forma electrónica, por lo tanto posee un contrato en digital y desea que Glenda, su clienta, lo firme de forma electrónica.

Como entendemos tanto Daniel quien da el servicio, como Glenda quien lo recibe deben poseer un juego de dos “llaves electrónicas” cada uno, una pública y otra privada. Por lo tanto Daniel le envía el contrato (1) a Glenda para que lo firme electrónicamente con su llave privada (2) que solamente ella conoce; al hacer esto Glenda regresa el documento electrónico con su firma digital, lo que implica que ella se obliga a lo plasmado en el contrato, en obediencia a los principios de autenticidad, integridad y no repudiación que rigen las actividades del uso de la firma electrónica.

Ahora Daniel debe verificar si su clienta lo firmó, por lo tanto usa su llave pública (3) que es la referencia de la llave privada de Glenda para poder comprobar su autenticidad (4).

Esta acción tiene la validez que formato tradicional; aunque existe la excepción de aquellos documentos jurídicos que según dicte otra ley, la carta magna o se requiera que estén almacenados, procesados y firmados de forma física (Art. 8 del anteproyecto de Ley de Firma Electrónica). Ejemplo de ello son los convenios interinstitucionales, de lo contrario, la acción de que Daniel haya enviado a Glenda el contrato y que sea firmado electrónicamente equivale a que lo haya hecho de forma física. Como también el valor probatorio de los documentos electrónicos privados (Art. 10 del anteproyecto de Ley de Firma Electrónica) con firma electrónica certificada que se refiera a actos jurídicos que estén dentro de la presente Ley de Firma Electrónica, de igual manera tienen el mismo valor jurídico que un documento en formato impreso.

» QUINTO: CERTIFICADOS DIGITALES

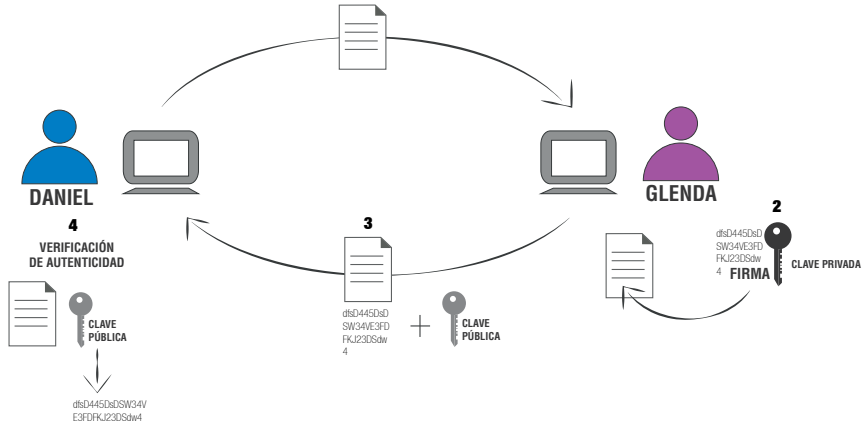
Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (el Proveedor de Servicios de Certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.

Este tipo de certificados se emplea para comprobar que una clave pública pertenece a un individuo o entidad. La existencia de firmas en los certificados aseguran por parte del firmante del certificado (el Proveedor de Servicios de Certificación) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.

Un aspecto fundamental es que el certificado para cumplir la función de identificación y autenticación necesita del uso de la clave privada (que sólo el titular conoce). El certificado y la clave pública se consideran información no sensible que puede distribuirse a terceros. El certificado sin más no puede ser utilizado como medio de identificación, pero es una pieza imprescindible en los protocolos usados para autenticar a las partes de una comunicación digital, al garantizar la relación entre una clave pública y una identidad.

Los componentes principales de un certificado digital son: 1) titular, 2) una llave pública, 3) emisor, y 4) período de validez.

PROCESO GRÁFICO DE FIRMA ELECTRÓNICA



Por ejemplo. Daniel quien tiene una empresa que brinda un servicio y cuyos contratos los hace de forma electrónica, por lo tanto posee un contrato en digital y desea que Glenda, su clienta, lo firme de forma electrónica.

Tanto Daniel quien da el servicio, como Glenda quien lo recibe deben poseer un juego de dos “llaves electrónicas” cada uno, una pública y otra privada, que no son más que códigos encriptados. Por lo tanto Daniel le

envía el contrato a Glenda lo firme electrónicamente con su llave privada que solamente ella conoce; al hacer esto Glenda regresa el documento electrónico con su firma.

Ahora Daniel debe verificar si su clienta firmó el documento digital, por lo tanto usa la llave pública que es la referencia de la llave privada de Glenda para poder comprobar su autenticidad. Esta acción es equivalente a documentos soportados electrónica con los de formato tradicional, la acción de que Daniel haya enviado a Glenda el contrato y que sea firmado electrónicamente equivale a que lo haya hecho de forma física. Como también el valor probatorio de los documentos electrónicos privados (Art. 10) con firma electrónica certificada que se refiera a actos jurídicos que estén dentro de la presente Ley de Firma Electrónica, de igual manera tienen el mismo valor jurídico que un documento en formato impreso.

No es equivalente la firma física con la electrónica en aquellos documentos jurídicos que según dicte otra ley, la carta magna o se requiera que esté de almacenados, procesados y firmados de forma física (Art. 8); como un ejemplo convenios interinstitucionales,

¿QUÉ TIPOS DE FIRMAS EXISTEN?

La Firma Electrónica que trata este documento, se refiere a dos grandes tipos:

Firma Electrónica Simple: es el tipo básico de firma electrónica. Es un conjunto de datos electrónicos unido a un documento y utilizado cuando un emisor envía un mensaje al receptor, y dicho mensaje va cifrado, de manera que nadie pueda modificarlo ni alterarlo. Además, la firma identifica al sujeto que la utiliza.

Firma Electrónica Certificada: al igual que la firma electrónica simple, este tipo de firma es un conjunto de datos electrónicos para identificar al emisor de un mensaje, al igual que la integridad del mismo.

Sin embargo, la diferencia con la firma electrónica simple es que este modelo de firma es creado bajo una serie de medios que están bajo el control directo del signatario o firmantes de la misma. Dicho de otro modo, es un método más seguro de autenticación e identificación del signatario, ya que únicamente el firmante controla los modos de creación de la misma.

PANORAMA REGIONAL DE LA LEGISLACIÓN DE FIRMA ELECTRÓNICA

PAÍSES	FIRMA ELECTRÓNICA Y DIGITAL	PERÍODO DE REFORMA
Argentina	Ley No. 25.506. Firma electrónica. Decreto No. 2628/2 Decreto No. 724/06	2007
Belice	Acta de Transición Electrónica	2003
Bermudas	Ley de Documentos, Firmas y Comercio Electrónico	1999
Bolivia (Estado Plurinacional de)	Ley 19.799 Firma electrónica, firma electrónica avanzada.	2007
Chile	Ley 527/1999 Del Comercio electrónico y de las firmas digitales.	2002
Colombia	Ley de Documentos, Firmas y Comercio Electrónico	1999
Costa Rica	La Ley 8454 de Firma digital, publicada el 13 de octubre de 2005. Sigue el Reglamento 33018-MICIT del 21 de abril de 2006	2005/2006
Ecuador	Ley No. 2002-67. El Banco Central del Ecuador representa la primera Entidad de Certificación de Información y Servicios.	2002
Guatemala	Decreto 47-2008, Ley para el reconocimiento de las comunicaciones y firma electrónica.	2008
México	Decreto 29/5/2000 Reforma del código comercial para que la firma digital obtuviera valor jurídico. La ley atribuye valor jurídico a los certificados de gobierno y a las transacciones electrónicas/digitales.	2001
Panamá	Ley 43 del 31 de julio del 2001	2000

PAÍSES	FIRMA ELECTRÓNICA Y DIGITAL	PERÍODO DE REFORMA
Perú	Ley 27269, Nuevo Reglamento de la Ley de Firmas y Certificados Digitales aprobado por Decreto Supremo 052-2008-PCM	
Puerto Rico	S.B. 423 (188) Digital Signature Acts	1998
Trinidad y Tobago	TheElectronicTransactions Bill, 2009	2009
Uruguay	Decreto 65/998 de fecha 10 de marzo de 1998	1998
Venezuela	Decreto Ley No. 1204 dictado el 10/02/01	2001

¿CUÁLES SON LOS PRINCIPIOS DE LA LEY DE FIRMA ELECTRÓNICA?

AUTENTICIDAD	Se transmite un mensaje confiable y esta garantía perdura a través del tiempo.
INTEGRIDAD	Se otorga certeza de que los datos recibidos por medios electrónicos no han sido modificados en su tránsito desde el iniciador hasta el destinatario.
CONFIDENCIALIDAD	Se garantiza al iniciador y destinatario que los mensajes electrónicos no serán conocidos por terceras personas sin su expresa autorización.
EQUIVALENCIA FUNCIONAL	Observar en los documentos archivados y comunicados electrónica mente aquellos requisitos que son exigidos en los documentos consignados en papel, con el fin de determinar la manera de satisfacer sus objetivos y funciones.
NO REPUDACIÓN	Se garantiza que cuando un mensaje ha sido suscrito con FEC, de conformidad a lo establecido en la presente ley, no puede ser repudiada su autoría por la persona del iniciador.

NEUTRALIDAD TECNOLÓGICA	Es la no discriminación de la información consignada en papel o de información comunicada o archivada electrónicamente.

CONCEPTUALIZANDO:

Firma digital: es un conjunto de métodos criptográficos y técnicos. Es un concepto fundamentalmente técnico.

Firma electrónica: es un término mucho más amplio y hace referencia a cuestiones legales, organizativas, técnicas, etc.

Es el que contiene el mensaje que se desea enviar “firmada” de un remitente a un destinatario.

Este proceso se conoce como encriptación por llave privada.

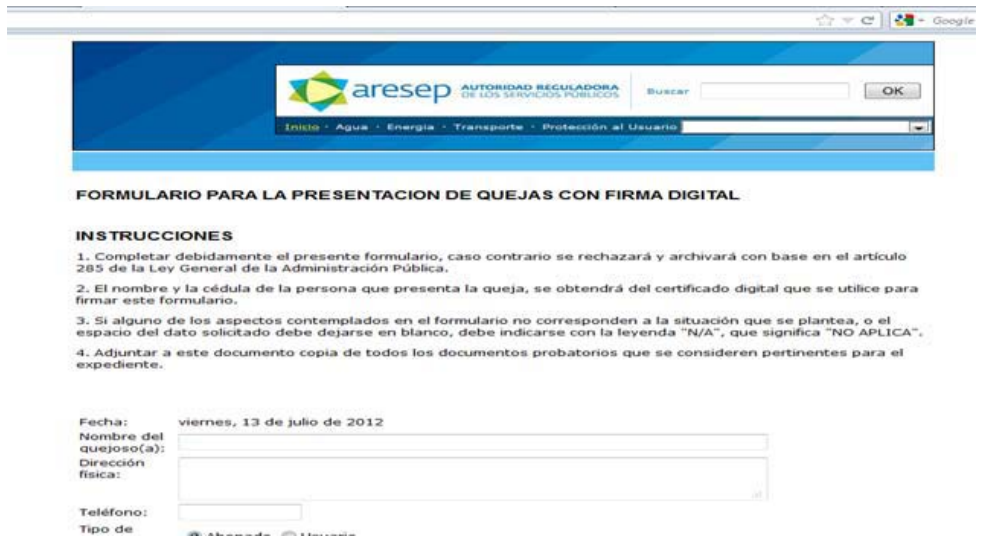
La firma electrónica certificada posee plena eficacia jurídica, siendo admitida como prueba en un juicio. Se equipara, por tanto, a la firma manuscrita, a sus efectos jurídicos y al valor probatorio de la misma.

Capítulo II

Aplicación de la Firma Electrónica

Ejemplos del uso de Firma Electrónica

CASO INTERNACIONAL: AUTORIDAD REGULADORA DE SERVICIOS PÚBLICOS (COSTA RICA)



La Autoridad Reguladora de Servicios Públicos de Costa Rica es la responsable de regular técnica y económicamente los mercados que la Ley 7593 y sus reformas le atribuyen, además de ser el garante de la

prestación óptima de los servicios respectivos para elevar la calidad de vida y la satisfacción de las necesidades de los habitantes de Costa Rica en forma transparente, oportuna, eficiente y razonable.

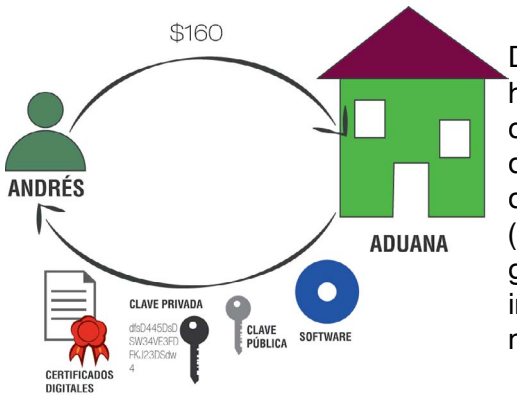
Actualmente la Autoridad recibe sus quejas y denuncias mediante un formulario expuesto en su sitio web: http://forms.aresep.go.cr/denuncias/

Antes del uso de firma digital, las personas podían solamente descargar el formulario, llenarlo, firmarlo y llevarlo a las instalaciones de la Autoridad, lo cual limitaba el servicio a las personas que por su ubicación, horario u obligaciones no pudieran presentarse. Mediante el desarrollo de la firma digital cualquier persona, desde cualquier lugar y en cualquier momento puede tener acceso a este servicio.

Los usuarios obtienen su firma electrónica por medio de los proveedores de certificación electrónica.

Fuente: Firma Digital, Costa Rica

CASO NACIONAL: TELEDESPACHO ADUANAL

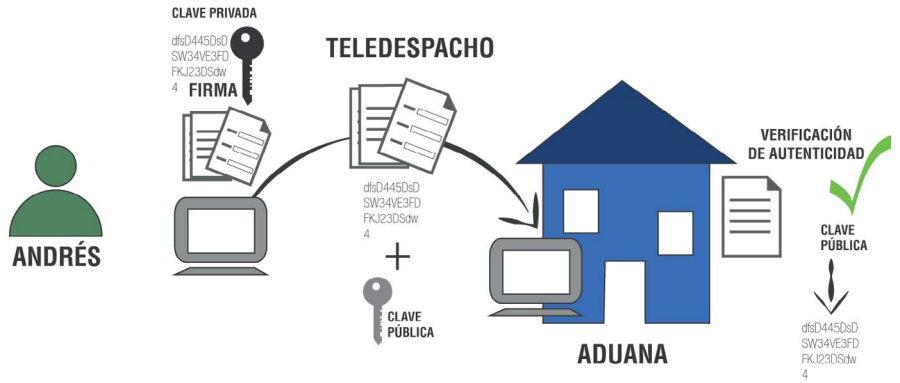


Desde enero del 2002} es posible hacer trámites reales por internet con la Dirección General de la Renta de Aduanas, en específico el envío de la Declaración de Mercancías (Póliza por internet), agilizando en gran medida el procesamiento de información para la importación de mercadería.

- Desarrollo de la Plataforma Tecnológica y Operativa de TELEDESPACHO,
- Servicios cerrados de emisión de Certificados Digitales,
- Software de Firma Digital, y
- Centro de Soporte.

GS1 El Salvador proporciona a su cliente (Andrés) el certificado digital que contiene la firma digital que necesita para firmar sus pólizas aduaneras (Agente Aduanal); este certificado digital es un CD que contiene la información necesaria para hacer efectiva su firma. Al introducir el CD, y como parte de los sistemas de seguridad, el certificado digital con toda la información sobre la firma electrónica privada se activa al incorporar un pin único y de conocimiento exclusivo del dueño de la firma electrónica (en este caso, del Agente Aduanal).

Una vez está firmada digitalmente la póliza (con la llave privada) se envía por el sistema de Teledespacho hacia Aduana, quienes por medio de un sistema de verificación de autenticidad (llave pública) verifican con el proveedor del certificado digital (GS1, cuya área se denomina CertiCámara) que la firma digital en la Póliza corresponde a la persona que dice ser.



PREGUNTAS SOBRE LA FIRMA ELECTRÓNICA

» USO DE LA FIRMA ELECTRÓNICA

¿Quiénes deben usar la firma electrónica?

Todos aquellos cuyas diligencias tengan el potencial de hacerse por medios tecnológicos, y/o que estén sujetas a las condiciones de sus contrapartes. Excepto los menos de edad e incapaces según reza la Ley. En otras palabras, para mayor eficiencia en el uso de la firma electrónica el firmante debe contar con los medios necesarios para poderlo hacer, como el tener el equipo y conocimiento adecuado (computadora, procesador

de texto, software de certificación, certificado electrónico) para dicho fin, además tanto el propietario del documento como el firmante deben tener las mismas condiciones tecnológicas para utilizar este tipo de firma.

Puedo yo, como persona natural, ¿utilizar firma electrónica certificada?

Sí, de hecho para ciertos trámites que involucren concesión de derechos, contrataciones, será necesario contar con una firma electrónica certificada, si así se requiere o acuerda entre las partes.

¿Estoy obligado a usar la firma electrónica simple o certificada?

No, no es una obligación, las partes pueden hacer uso de la Firma Electrónica o la manuscrita.

¿Puedo hacer uso indiscriminado de la firma electrónica y de mi firma manuscrita?

Sí, para ciertos documentos que requieren una solemnidad especificada en la Ley es necesario hacer uso de la firma manuscrita, sin que esto discrimine el uso de la firma electrónica en otros asuntos.

¿Quién emite las firmas electrónicas y los certificados digitales?

La Ley presenta la figura del Proveedor de Servicios de Certificación Electrónica, cuyo actuar, obligaciones y derechos están regulados por esta Ley y por la SIGET.

¿Debo tener o comprar un software especial para usar mi firma electrónica?

El proceso de obtención de una firma electrónica debería incluir el software y la capacitación en el uso; esto será regulado en el reglamento.

¿Tiene fecha de validez y caducidad la firma electrónica certificada y la simple?

Sí, los períodos de vigencia serán negociados entre el cliente y el Proveedor de Servicios de Certificación Electrónica bajo los lineamientos establecidos

por la Unidad de Firma Electrónica de la SIGET.

¿Los certificados digitales se vencen?

Sí, y es también tarea de la SIGET regular estos período bajo el acuerdo entre el cliente y el Proveedor de Servicios de Certificación Electrónica.

» DOCUMENTOS Y COMUNICACIONES ELECTRÓNICAS

¿Puedo firmar mis correos electrónicos electrónicamente?

Sí, los correos electrónicos son considerados como un mensaje de datos y su contenido puede ser firmado electrónicamente por el emisor.

¿Cómo puedo colocar la firma electrónica en un documento?

Para colocar una firma digital en un documento redactado por ejemplo en un procesador de texto u otro formato, se siguen estos pasos:

Paso 1: Se debe de contar con la firma electrónica certificada dentro de la computadora.

- Presionar “inicio”, seleccionar “Herramientas de Microsoft Office”.
- Seleccionar la opción “Certificado digital para proyectos VBA”.
- Se le debe colocar un nombre al certificado digital, normalmente se coloca el nombre del firmante y luego se presiona el botón de aceptar.

Paso 2: Haciendo esto se colocará la firma en un documento:

- Se abre el documento en el cual se colocará la firma electrónica.
- Luego seleccionar Archivo > Información > Proteger documento

- Y seleccionar la opción “Agregar una firma digital”, aparecerá una ventana a la cual se debe presionar “aceptar”
- Luego de esto aparecerá otra ventana donde se colocará “Razón para firmar esta documento” esto puede ser: “personal”, “Trámite”, entre otros.
- Seleccionar el botón “cambiar” donde escogeremos el certificado que se ha creado.
- Al realizar esta acción nos mostrará las características que posee el certificado digital, si es la primera vez que se configura la firma electrónica, aparecerá una leyenda que dice: “Este certificado raíz de la entidad de certificación no es de confianza…” es porque no se ha configurado nuestra firma electrónica. Para configurarlo:
- En esa misma ventana seleccionar la opción “Instalar certificado…”
- Nos abrirá un “Asistente de importación de certificados” a lo cual presionar el botón “siguiente”
- Nos pedirá identificar donde se encuentra el archivo de nuestra forma electrónica para colocarlo en su “Almacén de certificados” debemos seleccionar la opción “Colocar todos los certificados en el siguiente almacén” y presionar “Examinar…”
- Seleccionamos la carpeta donde se encuentra el archivo de la firma digital. Presionar “aceptar” y luego “Siguiente” y “Finalizar”
- Para confirmar que todo ha salido bien nos aparecerá un mensaje en una ventana emergente: “La importación se completó correctamente”
- Para confirmar que todo ha salido bien, en la ventana de las propiedades del certificado seleccionamos la pestaña de “detalles” y podemos ver claramente todas las propiedades. Y presionamos “aceptar”
- Al realizar estos pasos podemos ver que en la ventana donde iniciamos el proceso de firmar está habilitado el botón de “firmar” al cual lo presionamos. Al hacer esto aparecerá una ventana emergente donde dice: “Su firma se ha agregado correctamente al documento” y presionamos “aceptar”

¿Cómo sé que mi documento ya está firmado electrónicamente?

En las herramientas de redacción y lectura de textos, en la parte inferior de la pantalla de edición existe un icono de “sello” de color rojo que indica que el documento está firmado electrónicamente.

¿Qué tipo de documento puedo firmar electrónicamente?

Todos aquellos documentos que la Ley no exija una firma física (por ejemplo: actas de matrimonio, convenios, divorcios, herencias, etc.)

¿Puedo firmar electrónicamente un documento que he escaneado de un original?

El documento en sí no incluye la firma, sino más bien se le agrega la firma más el Algorítmo de Hash que unidos forman un código encriptado que acompaña al documento; es así que incluso un documento escaneado puede firmarse electrónicamente.

¿Necesito estar conectado a internet para hacer uso de mi firma electrónica?

No, ya que la firma electrónica funciona como un archivo que se guarda en la computadora.

¿Puedo quitar la firma electrónica de un documento una vez he aplicado mi firma electrónica?

Sí, las herramientas de edición de documentos que tienen la capacidad de colocar la firma electrónica dentro de un documento, también pueden quitarla siempre y cuando lo haga el emisor del documento original.

¿Para firmar un documento electrónicamente, éste debe estar en algún formato en especial (Word, Excel, PDF, etc.)?

Toda herramienta de procesamiento y edición de texto que tenga la funcionabilidad de realizar tal acción, como por ejemplo el paquete de

software Microsoft Office, Lotus Document, Adobe Acrobat (No así Adobe Acrobat Reader)

¿Debo usar la misma computadora para firmar electrónicamente un documento?

Como una buena práctica de seguridad y protección de su firma electrónica se debe realizar el proceso de la firma electrónica en la menor cantidad posible de computadoras. Existen otras opciones portátiles como el uso de "chip" donde se puede usar en varias computadoras y la firma electrónica no queda registrada en ellas.

» CONSERVACIÓN DE DOCUMENTOS

¿En qué formato se guardan mis documentos una vez firmados electrónicamente?

Se guardan en el mismo formato en que se crearon.

¿En qué dispositivos puedo guardar mis documentos firmados electrónicamente?

En memorias USB, discos duros externos, en una computadora, CD, e incluso puede contratar a un Proveedor de Servicios de Almacenamiento Tecnológico, nacional o extranjero siempre y cuando cumpla con las condiciones establecidas en esta Ley.

Quiero un resguardo de mis documentos firmados electrónicamente, ¿puede una empresa o un tercero guardarlos por mí?

Claro, los Proveedores de Servicios de Almacenamiento Tecnológico son una figura que la Ley permite para dar este servicio, tanto para personas naturales, jurídicas como para el Estado.

¿Cómo sabré que es una empresa legal y que tiene las condiciones para guardar la documentación?

La Unidad de Firma Electrónica velará porque los Proveedores de Servicios de Almacenamiento Tecnológico cumplan los requisitos de ley, incluyendo infraestructura, solvencia y operaciones. Estos aspectos están detallados en esta Ley.

¿Cómo puedo garantizar la autenticidad e integridad de la documentación que se va a almacenar?

El Art. 14 de esta Ley indica que todo documento que se requiera ser almacenado debe cumplir con requisitos para garantizar su autenticidad e integridad. Estos requisitos son: a) que los documentos electrónicos queden almacenados en forma íntegra, nítida, segura y con absoluta fidelidad, b) que pueda determinarse con precisión la fecha y la hora en las que un documento fue almacenado tecnológicamente, c) la recuperación del documento electrónico, y d) que cumpla con los reglamentos técnicos y normativos establecidas por la SIGET.

¿Puede una empresa extranjera almacenar mis documentos firmados electrónicamente?

Si, y sus servicios serán reconocidos en los mismo términos y condiciones exigidos por esta Ley cuando sean avalados por un prestador de servicio de almacenamiento tecnológico de documentos electrónicos nacionales.

» EMISIÓN Y RECEPCIÓN DE MENSAJES

¿Qué es un mensaje de datos?

Un mensaje de datos lo constituye la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, óptimos o similares, por ejemplo: correo electrónico, telegrama, mensaje de texto, etc.

Envié un mensaje de datos firmado electrónicamente ¿cómo puedo constatar que realmente el mensaje ha sido recibido por el destinatario?

Cuando el mensaje de datos ingrese al repositorio del destinatario, encontrándose a disposición de éste para su acceso; además, la comunicación dirigida al destinatario permitirá corroborar la recepción del mensaje de datos, y también se verificará la recepción cuando el iniciador pueda evidenciar que ha recibido su mensaje de datos. Por supuesto, las partes pueden establecer otros mecanismos de mutuo acuerdo.

» CERTIFICADOS DIGITALES Y FIRMA ELECTRÓNICA CERTIFICADA

¿Por qué debo tener una firma electrónica certificada y no una firma electrónica simple?

La firma electrónica certificada es indispensable para las transacciones que en la Ley se detallan de hacer exclusivo de este tipo de firma electrónica, la cual es respalda los proveedores de certificados digitales y la Superintendencia General de Electricidad y Telecomunicaciones; mientras que la firma electrónica simple se refiere a lo que comúnmente se usa, como pines de cajeros automáticos, transacciones en línea, etc.

¿Quiénes pueden hacer uso de la Firma Electrónica Simple y Certificada?

Toda persona, pero en especial los representantes de las personas jurídicas, los funcionarios y empleados públicos que tengan en su responsabilidad el otorgamiento de derechos e implementación de sanciones. A excepción de los menores de edad y de los que sean declarados incapaces.

Soy representante legal de una empresa y tengo a mi poder la firma electrónica certificada de la empresa, ¿puedo también tener una firma electrónica certificada personal?

Si, ya que en el certificado digital se hará mención de los alcances de la firma electrónica certificada, es decir, no podrá utilizarse una firma electrónica certificada de la cual la persona es responsable como representante legal de una empresa para fines personales, y viceversa.

¿Qué características tiene la firma electrónica certificada?

La firma electrónica certificada debe tener la garantía de que ésta sea inalterable, para ello tiene que estar sustentada en un método de creación y verificación confiable y seguro. Con respecto a la confiabilidad, la firma electrónica certificada debe pertenecer al titular de la misma, y el mensaje de datos con que está vinculado debe no haber sido modificado desde el momento de su envío, si el resultado del procedimiento de verificación así lo indica.

¿Qué debe cumplir mi documento electrónico firmado para poder conservarlo y utilizarlo nuevamente?

El Art. 11 establece que para este fin, el documento debe cumplir con tres condiciones: a) que contenga la firma electrónica certificada, b) que ésta no muestre ninguna alteración, y c) se pueda presentar en otro formato si se ha destruido o dañado el documento electrónico original.

¿Los certificados electrónicos son para firmas electrónicas certificadas y también para simples?

Son solamente para las firmas electrónicas certificadas porque uno de los atributos de esta es su garantía de legitimidad y las certificaciones electrónicas logran este propósito.

¿Qué información es la que contiene el certificado digital?

El certificado electrónico debe contener: identificación del titular incluyendo su dirección electrónica y domicilio; la identificación del proveedor de servicios de certificación que proporciona el certificado incluyendo su domicilio y dirección electrónica; fecha de la acreditación y caducidad asignada al proveedor de servicios por la SIGET; la fecha de emisión y expiración del certificado; número de serie o identificación del certificado; la firma electrónica certificada del prestador de certificación que emitió el certificado; datos de verificación de la firma que correspondan a los datos de creación de la firma bajo el control del firmante; indicación de la ruta de certificación, entre otros que se detallan en el Art. 59 del Anteproyecto de Ley de Firma Electrónica.

¿Por qué motivos se puede cancelar un certificado electrónico?

Existen tres motivos por los cuales los certificados electrónicos pueden ser cancelados: a) que se compruebe que alguno de los datos del certificado electrónico proporcionado por el proveedor de certificación es falso, b) que sea violentado el sistema de seguridad del proveedor de servicios de certificación que afecte la integridad y confiabilidad del certificado, y, c) que el signatario (cliente) de aviso al proveedor del hurto, destrucción o extravío del certificado electrónico.

¿Qué derechos tienen los usuarios de los servicios de firma electrónica certificada?

Los usuarios tienen 8 derechos que se ven expresados en el Art. 63, algunos de ellos son: a) ser informador por los proveedores de servicios de certificación de las características generales de los procedimiento de creación y de verificación de firma electrónica certifica, así como las reglas sobre prácticas de certificación, b) a traspasar sus datos a otro prestador de servicios de certificación y de almacenamiento tecnológico de documentos electrónicos si así lo solicitan, etc.

¿Qué obligaciones tienen los usuarios de los servicios de firma electrónica certificada?

Los usuarios o titulares de firmas electrónicas certificadas y de almacenamiento tecnológico de documentos electrónicos quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a:

a) brindar declaraciones veraces y completas,

b) custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el prestador y a actualizar sus datos en la medida que éstos vayan cambiando, so pena de pagar por la indemnización de daños y perjuicios derivada del incumplimiento de estas obligaciones, y

c) solicitar oportunamente la suspensión o revocación del certificado ante cualquier circunstancia que pueda haber comprometido la privacidad de los datos de creación de firma electrónica certificada.

» USO DE LA FIRMA ELECTRÓNICA CERTIFICADA ANTE Y POR EL ESTADO

¿Puedo usar mi firma electrónica certificada en los trámites con el Estado?

Si, pero el uso de firma electrónica certificada de una persona en la interacción con el Estado sólo será necesaria en casos de suscripción de contratos o cuando la ley expresamente exija ese requisito.

Soy empleado/funcionario público, ¿Cuándo puedo usar mi firma electrónica simple en los trámites al interior del Estado?

Sólo en los casos de aquellos que presten servicios públicos, ejecuten o realicen actos administrativos dentro de su ámbito de competencia.

Soy empleado/funcionario público, ¿Cuándo puedo usar mi firma electrónica certificada en los trámites al interior del Estado?

De hecho es obligación usar la firma electrónica certificada cuando los empleados/funcionarios expidan cualquier documento o realicen actos administrativos en los que se otorguen derechos o sanciones a los administrados. Ahora bien, cuando la Constitución o la Ley exija alguna solemnidad que no sea susceptible de cumplirse mediante documentos electrónicos, mensaje de datos o firmas electrónicas certificadas, se exceptuará el uso de la firma electrónica certificada.

¿Podrán las instituciones de gobierno contratar los servicios de los Proveedores de Servicios de Almacenamiento?

Efectivamente, las instituciones del Estado podrán conservar, registrar y archivar cualquier información y/o actuación por medios electrónicos, los cuales sustituirán a los registros físicos para todo efecto, y también podrá contratar a cualquier prestador de servicios de almacenamiento tecnológico de documentos electrónico cuando éste último cumpla las condiciones técnicas y legales de esta Ley y de sus reglamentos.

» UNIDAD DE CONTROL Y VIGILANCIA

¿Quién regulará y vigilará a los proveedores de certificación electrónica y a los de almacenamiento?

Será la Unidad de Firma Electrónica, que se creará en el seno de la Superintendencia General de Electricidad y Telecomunicaciones (SIGET).

¿Quién aprobará las tarifas que los proveedores cobre en concento de certificación electrónica y almacenamiento?

Según el Art. 38 de la Ley, la SIGET, por medio de su Junta de Directores, aprobará el pliego tarifario de los servicios a que se refiere la Ley y que se brindarán a los usuarios. Es decir, la SIGET aprobará el pliego tarifario que sea presentado por los proveedores de los servicios a los que se refiere la Ley, el cual se establecerá empleando un modelo basado en costos, no discriminatorios y transparentes, de acuerdo a la metodología que se establezca en el reglamento.

¿El listado de proveedores será público?

La SIGET además creará la Sección de los Proveedores de Servicios de Certificación y de los Prestadores de Servicios de Almacenamiento Tecnológico de Documentos Electrónicos dentro del Registro de Electricidad y Telecomunicaciones (que está adscrito a la SIGET). La información de la Sección será pública atendiendo a las medidas de resguardo y conservación que amerite la misma.

¿Podrá la SIGET por medio de la Unidad de Firma Electrónica emitir normas técnicas, estándares u otras medidas de obligatorio cumplimiento por los proveedores de certificación electrónica y de almacenamiento?

Si, para el correcto cumplimiento de las atribuciones concedidas por la Ley, la SIGET, realizará (por su medio o por contratación), auditorías de los proveedores de certificación y de almacenamiento tecnológica. Además podrá adoptar las medidas preventivas necesarias para garantizar la confiabilidad de los servicios prestados a los proveedores; esto incluye el dictado de normas técnicas, medidas, el uso estándares o prácticas internacionales.

» PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA Y PROVEEDORES DE ALMACENAMIENTO TECNOLÓGICO

¿Cuáles son las actividades que la Ley le permite a los proveedores de servicios de almacenamiento tecnológico?

El Art. 54 detalla tres actividades que podrán realizar los prestadores de servicios de almacenamiento tecnológico: a) ofrecer los servicios de procesamiento y almacenamiento tecnológico de documentos electrónicos, b) ofrecer los servicios de archivo y conservación de documentos almacenados tecnológicamente, y c) cualquier otra actividad a fín, relacionada con el almacenamiento tecnológico de documentos electrónicos.

¿Cuáles son las obligaciones de los proveedores de servicios de certificación electrónica?

El detalle de las obligaciones está dado en el Art. 49 de la Ley, siendo algunas de ellas la de adoptar las medidas necesarias para determinar la exactitud de los certificados electrónicos que proporcionen, la identidad y la calidad del signatario, y la garantía de la validez, vigencia, legalidad y seguridad del certificado electrónico que proporcione, entre otras.

Si un proveedor se retira del mercado, ¿podrá pasar la información a otro proveedor de mi preferencia? ¿deberé pagar por ello?

Si, una vez ha completado todo el proceso de cese de actividades que la Ley establece en el Art. 52, los proveedores (sean de certificación o de almacenamiento tecnológico) trasladarán sus usuarios activos a otro prestados con la finalidad de garantizar la continuidad de servicio hasta la finalización del contrato, previo consentimiento expreso del usuario, sin que signifique costo adicional para el usuario.

¿Cuáles son las obligaciones de los proveedores de almacenamiento tecnológico?

Estos proveedores tendrán la obligación de emplear personal calificado en temas de almacenamiento tecnológico, contar con sistemas confiables,

garantizar la protección, la confidencialidad y el debido uso de la información suministrada por el usuario del servicio, contar con un plan de contingencia que garantice la prestación continua de sus servicios, y utilizar sistemas confiables para almacenar los documentos electrónicos; mayores detalles están en el Art. 55 de la Ley.

¿Existen multas o sanciones para los proveedores que incumplan la Ley?

Si, los proveedores (de certificación y de almacenamiento tecnológico) están sujetos al régimen sancionador que estable la Ley en el Art. 66: infracciones leves, graves y muy graves.

Capítulo III

Anteproyecto de Ley de Firma Electrónica

Anteproyecto de Ley de Firma Electrónica

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR,

CONSIDERANDO

I. Que el Art. 101 de la Constitución de la República establece que el Estado debe promover el desarrollo económico y social mediante el incremento de la producción, la productividad y la racional utilización de los recursos. En consecuencia, debe crear los instrumentos legales que propicien el uso de tecnologías de información y comunicaciones;

II. Que el Art. 2 de la Constitución de la República reconoce que toda persona tiene el derecho a la seguridad jurídica; por lo que el Estado debe crear un marco legal que brinde seguridad a los usuarios de las comunicaciones electrónicas y a las transacciones autorizadas mediante las aplicaciones de la tecnología o la suscripción electrónica de las mismas, brindándoles validez jurídica; y,

III. Que el desarrollo de las tecnologías de información y comunicación se ha convertido en un factor estratégico que mejora la eficiencia de la educación, fomentando la competitividad y el crecimiento económico de los pueblos; asimismo, eleva la calidad de vida de los ciudadanos, al permitir la inclusión de más personas al sistema productivo, razón por la cual nuestro país, por medio de la presente Ley, pretende promocionar el uso de tales tecnologías para propiciar el comercio y el desarrollo económico, incorporándolo al entorno mundial en el que se producen interacciones seguras, dentro de la sociedad de la información.

POR TANTO,

en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Economía,

DECRETA la siguiente:

LEY DE FIRMA ELECTRÓNICA

TÍTULO I: DISPOSICIONES GENERALES

» CAPÍTULO I: OBJETO Y ALCANCE

Objeto.

Art. 1.- La presente Ley tiene por objeto:

a) Equiparar la firma electrónica simple y firma electrónica certificada con la firma autógrafa;

b) Otorgar y reconocer eficacia y valor jurídico a la firma electrónica certificada, a los mensajes de datos y a toda información en formato electrónico que se encuentren suscritos con una firma electrónica certificada, independientemente de su soporte material; y,

c) Regular y fiscalizar lo relativo a los proveedores de servicios de certificación electrónica, certificados electrónicos y proveedores de servicios de almacenamiento de documentos electrónicos.

Neutralidad tecnológica y equivalencia funcional.

Art. 2.- Las regulaciones de la presente Ley serán aplicables a la comunicación electrónica, firma electrónica certificada y firma electrónica simple o cualquier formato electrónico, independientemente de sus características técnicas o de los desarrollos tecnológicos que se produzcan en el futuro; sus normas serán desarrolladas e interpretadas progresivamente, siempre que se encuentren fundamentadas en neutralidad tecnológica y equivalencia funcional.

» CAPÍTULO II: DEFINICIONES Y PRINCIPIOS GENERALES

Definiciones.

Art. 3.- Para los efectos de la presente Ley, se utilizarán las siguientes definiciones:

Acreditación: Es la autorización que otorga la Superintendencia General de Electricidad y Telecomunicaciones, SIGET, a los proveedores de servicios de certificación para operar y proporcionar certificados electrónicos y a los proveedores de servicios de almacenamiento de documentos electrónicos, una vez cumplidos los requisitos y condiciones establecidos en la presente Ley;

Certificado Electrónico: Documento proporcionado por un proveedor de servicios de certificación que otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con dicha firma;

Comunicación Electrónica: Toda información o mensajes de datos generado, enviado, recibido, archivado o comunicado por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos, EDI, el correo electrónico y otros;

Destinatario: La persona designada por el emisor para recibir el mensaje de datos, pero que no esté actuando a título de Intermediario con respecto a dicho mensaje;

Documento Electrónico: Todo mensaje de datos enviado, recibido o archivado por medios electrónicos, ópticos o de cualquier otra tecnología que forman parte de un expediente electrónico;

Firma: Comprenderá la firma electrónica simple y la firma electrónica certificada;

Firma Electrónica Simple: Son los datos en forma electrónica consignados en un mensaje de datos o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;

Firma Electrónica Certificada: Son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos;

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona que representa;

Iniciador de un Mensaje de Datos: Se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;

Proveedor de Servicios de Certificación: Persona jurídica autorizada por la SIGET, dedicada a emitir certificados electrónicos y demás actividades previstas en esta Ley;

Proveedor de Servicios de Almacenamiento Tecnológico de Documentos Electrónicos: Persona jurídica autorizada por la SIGET que, por la naturaleza de su negocio, brinda servicios de almacenamiento tecnológico de documentos electrónicos;

Signatario: Persona que posee un dispositivo de creación de firma y que actúa en nombre propio o a nombre de una persona natural o jurídica que representa;

SIGET: Superintendencia General de Electricidad y Telecomunicaciones.

Principios generales.

Art. 4.- Las actividades reguladas por esta Ley se regirán bajo los siguientes principios:

a) Autenticidad, con el cual se garantiza que el mensaje es confiable y esta garantía perdura a través del tiempo.

b) Integridad, por medio del cual se otorga certeza que los datos recibidos por medios electrónicos no han sido modificados en su tránsito desde el iniciador hasta el destinatario.

c) Confidencialidad, por medio del cual se garantiza al iniciador y destinatario que los mensajes electrónicos no serán conocidos por terceras personas, sin su expresa autorización.

d) Equivalencia Funcional, consiste en observar en los documentos archivados y comunicados de manera electrónica, aquellos requisitos que son exigidos en los documentos presentados por escrito y consignados en papel, con el fin de determinar la manera de satisfacer sus objetivos y funciones.

e) No Repudiación, por medio del cual se garantiza que cuando un mensaje ha sido suscrito con firma electrónica certificada, de conformidad a lo establecido en la presente Ley, no puede ser repudiada su autoría por la persona del iniciador.

f) Neutralidad tecnológica: Es la no discriminación entre la información consignada en papel y la información comunicada o archivada electrónicamente, siempre que cumpla con los requisitos establecidos en la presente Ley.

Tratamiento de Datos Personales.

Art. 5.- El tratamiento de los datos personales que precisen los prestadores de servicios de certificación y los prestadores de servicio de almacenamiento tecnológico de documentos electrónicos, para el desarrollo de sus actividades, se sujetarán a las siguientes reglas:

a) Para la expedición de certificados electrónicos al público y para el almacenamiento tecnológico de documentos electrónicos, los prestadores de servicios únicamente podrán recabar datos personales directamente de los firmantes. Se prohíbe que se cedan los datos personales de los usuarios.

b) Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de servicios en relación con la firma electrónica certificada. El titular podrá solicitar la rectificación o cancelación de los datos personales, cuando éstos fueren inexactos o incompletos.

c) Los proveedores de servicios de certificación y de almacenamiento de datos estarán obligados a revelar cualquier información, incluso la identidad de los contratantes, a solicitud del juez competente o de la Fiscalía General de la República, en el ejercicio de sus

funciones.

d) El responsable del registro de datos y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, estarán obligados a la confidencialidad de los mismos y al deber de guardarlos. Obligaciones que subsistirán aún después de finalizar sus relaciones con el responsable del registro de datos, con excepción de lo establecido en el literal anterior.

» CAPÍTULO III: EQUIVALENCIA Y VALOR JURÍDICO DE LA FIRMA ELECTRÓNICA

Equivalencia y valor jurídico de la Firma Electrónica Simple.

Art. 6.- La firma electrónica simple se tendrá por jurídicamente equivalente a la firma autógrafa. En cuanto a sus efectos jurídicos, la firma electrónica simple no tendrá validez probatoria en los mismos términos a los concedidos por esta Ley a la firma electrónica certificada; sin embargo, podrán constituir un elemento de convicción conforme a las reglas de la sana crítica.

TÍTULO II: MENSAJES DE DATOS Y DOCUMENTOS ELECTRÓNICOS

» CAPÍTULO I: DISPOSICIONES GENERALES

Equivalencia funcional.

Art. 7.- El mensaje de datos utilizando firma electrónica certificada, cualquiera que sea su medio de transmisión o de almacenamiento, se tendrá por jurídicamente equivalente al contenido de aquéllos emitidos de manera convencional; es decir, que se otorguen, almacenen o se transmitan por medios físicos. Los documentos almacenados tecnológicamente conforme a esta Ley y las reproducciones debidamente certificadas, tendrán el mismo valor jurídico que los documentos originales, se someterán al régimen legal de los originales y podrán ser impugnados de la misma manera que éstos.

Equivalencia de los documentos en soporte electrónico.

Art. 8.- Los documentos en soporte electrónico tendrán el mismo valor que los consignados de manera tradicional. Quedan exentos aquellos documentos o actos jurídicos que para su perfeccionamiento requieren formalidades y solemnidades especiales.

Documentos públicos emitidos en soportes electrónicos.

Art. 9.- Los documentos públicos emitidos por las instituciones estatales podrán estar contenidos en soporte electrónico y tendrán el valor asignado por el ordenamiento legal para esta clase de documentos.

Valor probatorio de los documentos privados electrónicos.

Art. 10.- Cuando el documento privado fuera generado con firma electrónica certificada y se refiera a actos jurídicos que no se encuentren excluidos por la presente Ley, el valor será el mismo que el reconocido en manera tradicional.

Conservación de documentos.

Art. 11.- Si de acuerdo al acto jurídico o por disposiciones del ordenamiento legal, se exige que la información sea conservada en la forma en que originalmente ha sido emitida, se entenderá que un documento electrónico cumple dicha exigencia, si la firma electrónica certificada demuestra que el documento no ha sido alterado.

Los documentos podrán ser presentados en un soporte diferente, en caso de destrucción del soporte electrónico que lo contenía originalmente.

Formas de conservación de documentos.

Art. 12.- El cumplimiento de la obligación de conservar documentos, registros o informaciones en documentos electrónicos, se podrá realizar por cuenta propia o a través de terceros.

Toda persona jurídica, nacional o extranjera, que realice almacenamiento tecnológico de documentos electrónicos de terceros, deberá registrarse como prestador de servicios de almacenamiento de documentos electrónicos ante la SIGET.

Las personas naturales y jurídicas que realicen por cuenta propia el almacenamiento de documentos electrónicos, con el interés que dichos documentos tengan el valor legal otorgado por esta Ley, deberán cumplir con los requisitos mínimos establecidos en la misma, su Reglamento y en las Normas o Reglamentos Técnicos que se emitan al efecto.

Requisitos para la Conservación de Documentos.

Art. 13.- Si la Ley requiere que la información contenida en un mensaje de datos conste por escrito, ese requisito se dará por cumplido, si la información que contiene el mensaje de datos está disponible para una consulta ulterior.

Cuando la Ley exige que ciertos actos o negocios jurídicos consten por escrito y que su soporte permanezca accesible, conservado o archivado por un periodo determinado de tiempo o en forma permanente, esto se podrá cumplir mediante un archivo electrónico, sólo si el mismo cumple con los siguientes requisitos:

1. Que la información que contenga pueda ser consultada posteriormente.

2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.

3. Que se conserve todo dato que permita determinar el origen y el destino del mensaje de datos, la fecha y la hora en que fue enviado o recibido.

Garantías mínimas que debe cumplir el sistema de almacenamiento tecnológico.

Art. 14.- Al someterse el documento a almacenamiento tecnológico, éste deberá quedar conservado en un medio adecuado. El procedimiento utilizado para el almacenamiento de documentos electrónicos deberá garantizar:

1. Que los documentos electrónicos queden almacenados en forma nítida, íntegra, segura y con absoluta fidelidad.

2. Que pueda determinarse con precisión la fecha y la hora en las que un documento fue almacenado tecnológicamente.

3. La recuperación del documento electrónico.

4. Que cumple con los reglamentos técnicos y normativas establecidas por la SIGET.

La omisión de cualquiera de estos requisitos, así como la alteración o adulteración que afecten la integridad del soporte o documento electrónico en el que la información ha sido almacenada, harán perder el valor legal que esta Ley otorga a los documentos almacenados tecnológicamente.

Declaración de prácticas de almacenamiento de documentos.

Art.15.-Toda persona jurídica que realice el almacenamiento de documentos electrónicos para terceros, redactará una declaración de prácticas de almacenamiento, en la que detallará, dentro del marco de esta Ley y de su Reglamento, la siguiente información:

1. Las obligaciones que se comprometen a cumplir en relación con la gestión de documentos almacenados tecnológicamente.

2. Las condiciones aplicables a la solicitud, conversión y almacenamiento de documentos electrónicos.

3. Las medidas de seguridad técnica y organizativa.

4. El resultado obtenido de la última auditoría del sistema de almacenamiento tecnológico de documentos electrónicos.

5. Los límites de responsabilidad para realizar el almacenamiento tecnológico de documentos electrónicos.

6. La lista de normas y procedimientos de almacenamiento tecnológico de documentos electrónicos.

7. Cualquier otra información que la Unidad de Firma Electrónica de SIGET solicite mediante Normas y Reglamentos Técnicos.

La declaración de prácticas de almacenamiento de documentos electrónicos, será proporcionada a la SIGET para su aprobación y deberá de estar disponible al público por vía electrónica o por cualquier otro medio y de forma gratuita.

Certificación de documentos electrónicos.

Art. 16.- Las reproducciones, microfichas, discos o certificaciones que resultaren de la utilización de algún sistema de almacenamiento tecnológico de documentos electrónicos permitido por esta Ley, serán certificados por el responsable del archivo u oficina, pública o privada, que ostenta la custodia.

Reconocimiento de documentos almacenados en el extranjero.

Art. 17.- Los documentos electrónicos almacenados por un prestador de servicio de almacenamiento extranjero, que brinde los servicios de almacenamiento tecnológico de documentos electrónicos, podrán ser reconocidos en los mismos términos y condiciones exigidos por esta Ley, cuando sean avalados por un prestador de servicio de almacenamiento tecnológico de documentos electrónicos nacional.

Supervisión y Control.

Art. 18.- Todo prestador de servicios de almacenamiento tecnológico de documentos electrónicos que brinde servicios a terceros, quedará sujeto a las facultades de supervisión y control de la Unidad de Firma Electrónica de SIGET, para los efectos de velar por el cumplimiento de las obligaciones correspondientes que establece esta Ley y su Reglamento.

» CAPÍTULO II: DE LA EMISIÓN Y RECEPCIÓN DE LOS MENSAJES DE DATOS

Verificación de la emisión del Mensaje de Datos.

Art. 19.- Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

a) El propio iniciador o la persona que lo representa, cuando en el documento conste su firma electrónica certificada.

b) Por un sistema de información programado por el iniciador, o bajo su autorización, para que opere automáticamente.

Reglas para la determinación del recibo del mensaje.

Art. 20.- Se presumirá el recibo del mensaje, cuando se comprobare por el sistema de recepción y tendrá lugar cuando el mensaje de datos ingrese

al repositorio del destinatario, encontrándose a disposición de éste para su acceso.

Lugar de emisión y recepción.

Art. 21.- De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo; y si no hubiere, se aplicará el domicilio que conste en el registro del proveedor de servicios de certificación y en su defecto, el designado por el derecho común.

Del acuse de recibo.

Art. 22.- Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

1. Toda comunicación del destinatario, automatizada o no; o,
2. Todo acto del destinatario, que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado, en tanto que no se haya recibido el acuse de recibo.

TÍTULO III: FIRMA ELECTRÓNICA CERTIFICADA Y CERTIFICADOS ELECTRÓNICOS

» CAPÍTULO I: DISPOSICIONES GENERALES

Requisitos y efectos de la firma electrónica certificada.

Art. 23.- La firma electrónica certificada debe estar sustentada en un método de creación y verificación confiable y seguro, de manera que aquélla sea inalterable, alertando al destinatario en caso de modificación

de la información, después de ser suscrita por el signatario.

La firma electrónica certificada tiene los siguientes efectos:

a) Vincula un mensaje de datos con su titular de manera exclusiva;

b) Permite la verificación inequívoca de la autoría e identidad del signatario;

c) Asegura que los datos de la firma estén bajo control exclusivo del signatario.

Efectos jurídicos probatorios.

Art. 24.- La firma electrónica certificada tendrá igual validez y los mismos efectos jurídicos y probatorios que una firma manuscrita, en relación con los datos consignados en un documento o mensaje de datos electrónicos en que fuere empleada.

En todo caso, al valorar la fuerza probatoria de un documento electrónico, se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado, comunicado y en la que se haya conservado la integridad de la información.

Presunciones del empleo de la firma electrónica certificada.

Art. 25.- El empleo de la firma electrónica certificada que cumpla los requisitos exigidos en la presente Ley, salvo prueba en contrario, presume lo siguiente:

a) Que la firma electrónica certificada pertenece al titular de la misma; y,

b) Que el mensaje de datos vinculado a la firma electrónica certificada no ha sido modificado desde el momento de su envío, si el resultado del procedimiento de verificación así lo indica.

Quienes no pueden hacer uso de firma electrónica certificada.

Art. 26.- No podrán solicitar certificados electrónicos y hacer uso de la firma electrónica certificada los menores de edad y los incapaces.

Uso de la firma electrónica certificada por representantes de personas naturales.

Art. 27.- Para los mandatarios de las personas naturales, sólo se utilizará la firma electrónica certificada de aquél, previa verificación de tal calidad por parte del proveedor de servicios de certificación, a través de la presentación de los documentos legales pertinentes de conformidad al ordenamiento jurídico, que acrediten tal calidad, circunstancia que deberá constar en el certificado que se le extienda, así como los límites de sus facultades.

Uso de la firma electrónica certificada por representantes de personas jurídicas.

Art. 28.- Los certificados electrónicos de personas jurídicas para los dispositivos electrónicos utilizados en una empresa, como computadoras, servidores, entre otros, deberán ser solicitados por medio de sus administradores y representantes legales con poder suficiente.

La custodia de los datos de creación de firma electrónica certificada asociados a cada certificado electrónico de persona jurídica, será responsabilidad de la persona natural solicitante, cuya identificación se incluirá en el certificado electrónico.

La persona jurídica podrá imponer los límites que considere, por razón de cuantía o materia, para el uso de los datos de creación de firma electrónica certificada. Estos límites deberán figurar en el certificado electrónico.

Se entenderán realizados por la persona jurídica los actos en los que su firma electrónica certificada se hubiera empleado, dentro de los límites establecidos. Si la firma electrónica certificada se utiliza transgrediendo dichos límites, la persona jurídica quedará vinculada frente a terceros y se aplicará lo establecido en el Código Civil.

» CAPÍTULO II: USO DE LA FIRMA ELECTRÓNICA CERTIFICADA POR LOS ÓRGANOS DEL ESTADO

Uso de firma electrónica simple.

Art. 29.- Los funcionarios y empleados del Estado que presten servicios públicos, ejecuten o realicen actos administrativos dentro de su ámbito de competencia, podrán suscribirlos por medio de firma electrónica simple.

Uso de Firma electrónica certificada.

Art. 30.- En aquellos casos en que los funcionarios o empleados del Estado expidan cualquier documento o realicen actos administrativos en que se otorguen derechos o sancionen a los administrados, será necesario utilizar firma electrónica certificada. El proveedor de servicios de certificación deberá consignar en el certificado la calidad con la que firmará electrónicamente y así como los límites de su competencia.

Se exceptúan del uso de la firma electrónica certificada, en aquellas actuaciones para las cuales la Constitución de la República o las Leyes exijan alguna solemnidad que no sea susceptible de cumplirse mediante documentos electrónicos, mensaje de datos o firmas electrónicas certificadas.

Validez de actos y contratos.

Art. 31.- Los actos y documentos de las instituciones del Estado que tengan la calidad de instrumento público, podrán suscribirse mediante firma electrónica certificada.

Interacción electrónica entre administrados y funcionarios públicos.

Art. 32.- Los administrados podrán relacionarse o comunicarse con las instituciones del Estado, sin necesidad de firma electrónica certificada, siempre que se ajusten a las técnicas y medios electrónicos establecidos para tal fin.

Actos de comunicaciones.

Art. 33.- Cualquier institución del Estado, siempre y cuando cuente con la infraestructura tecnológica adecuada, deberá realizar comunicaciones por vía electrónica, utilizando firma electrónica simple, de actos tales como citaciones y notificaciones, siempre y cuando el destinatario de los servicios públicos hubiera autorizado ese medio de comunicación. Dicha autorización surtirá efecto mientras el destinatario no comunique una modificación al respecto.

Conservación, registro y archivo.

Art. 34.- Las instituciones del Estado podrán disponer la conservación, registro y archivo de cualquier actuación que esté bajo su competencia, por medio de sistemas electrónicos. Tales archivos y registros sustituirán a

los registros físicos para todo efecto, debiéndose cumplir para ello con los requisitos establecidos en esta Ley y demás leyes pertinentes.

El Estado podrá contratar a cualquier prestador de servicios de almacenamiento tecnológico de documentos, que cumpla con las condiciones técnicas y legales establecidas en esta Ley, su Reglamento y en las Normas y Reglamentos Técnicos.

» CAPÍTULO III: DE LA AUTORIDAD COMPETENTE

La Autoridad de Control y Vigilancia.

Art. 35.- Créase la Unidad de Firma Electrónica, como parte de la Superintendencia General de Electricidad y Telecomunicaciones, SIGET. El Superintendente nombrará al funcionario que estará a cargo de esta Unidad, quien deberá reunir los mismos requisitos que para ser Directores, que se encuentran consignados en la Ley de Creación de la Superintendencia General de Electricidad y Telecomunicaciones.

De la Unidad de Firma Electrónica.

Art. 36.- La Superintendencia General de Electricidad y Telecomunicaciones, por medio de la Unidad de Firma Electrónica, será la competente para la acreditación, control y vigilancia de los proveedores de los servicios de certificación electrónica y de almacenamiento tecnológico de documentos electrónicos, de conformidad con esta Ley, su Reglamento y las Normas y Reglamentos Técnicos.

Competencias de la Unidad de Firma Electrónica.

Art. 37.- La SIGET, por medio de la Unidad de Firma Electrónica, tendrá las siguientes competencias:

1) Elaborar las normas y los reglamentos técnicos que sean necesarios para la implementación de la presente Ley.

2) Otorgar la acreditación a los proveedores de servicios de certificación y a los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, una vez cumplidas las formalidades y requisitos de esta Ley, su Reglamento y demás normas y reglamentos técnicos aplicables.

3) Validar los certificados electrónicos emitidos a favor de los

proveedores de servicios de certificación y de almacenamiento tecnológico de documentos electrónicos.

4) Verificar e inspeccionar que los proveedores de servicios de certificación y los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, cumplan con los requisitos contenidos en la presente Ley, su Reglamento, así como en normas y reglamentos técnicos aplicables.

5) Supervisar las actividades de los proveedores de servicios de certificación y los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, conforme a lo dispuesto en esta Ley y su Reglamento.

6) Imponer, recaudar y administrar las tasas establecidas en la ley.

7) Imponer las sanciones establecidas en la presente Ley.

8) Imponer, recaudar y administrar las multas establecidas en la ley.

9) Coordinar y representar al país frente a los organismos nacionales o internacionales sobre cualquier aspecto relacionado con el objeto de esta Ley.

10) Instruir de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a esta Ley.

11) Informar de oficio a la Fiscalía General de la República, cuando tenga indicios de un delito.

12) Requerir de los proveedores de servicios de certificación y a los prestadores de servicios de almacenamiento tecnológico de documentos, o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.

13) Mantener acuatizado en la página web institucional el listado de los prestadores de servicios de certificados y de almacenamiento tecnológico de documentos electrónicos y hacer publicaciones.

14) Presentar al menos un informe anual de su gestión, en el marco de esta Ley, al Ministerio de Economía o cuando éste lo requiera.

15) Definir y realizar los procedimientos para la recepción y resolución de denuncias.

16) Las demás que establezca la presente Ley y su Reglamento.

Aprobación de tarifas.

Art.38- La SIGET, por medio de su Junta de Directores, aprobará el pliego tarifario de los servicios a que se refiere esta Ley y que se brindarán a los usuarios.

La SIGET aprobará el pliego tarifario que sea presentado por los proveedores de los servicios a que se refiere esta Ley, el cual deberá establecerse empleando un modelo basado en costos, no discriminatorios y transparentes, de acuerdo a la metodología que se establezca en el Reglamento de esta Ley.

Registro de Electricidad y Telecomunicaciones.

Art. 39.- Créase dentro del Registro de Electricidad y Telecomunicaciones, adscrito a la SIGET, la Sección de los Proveedores de Servicios de Certificación y de los Prestadores de Servicios de Almacenamiento Tecnológico de Documentos Electrónicos, que deberá ser actualizada y custodiada por tal Registro. La información será pública.

Auditorías e Inspecciones.

Art. 40.- Para el correcto cumplimiento de las atribuciones concedidas por esta Ley, la SIGET realizará, directamente o por contratación, auditorías de los proveedores de servicios de certificación y a los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos.

Tasas.

Art. 41.- La tasa aplicable a los proveedores de servicios de certificación y de los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, será cobrada por la SIGET anualmente, siendo la tasa aplicable la del uno por ciento del valor de sus activos.

Los proveedores de servicios de certificación y los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, constituidos por instituciones del Estado, debidamente acreditados, estarán exentos del pago de las tasas previstas en este artículo.

Medidas para garantizar los servicios de certificación.

Art. 42.- La SIGET podrá adoptar las medidas preventivas necesarias para garantizar la confiabilidad de los servicios prestados por los proveedores de servicios de certificación y de los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos. A tal efecto, podrá dictar las normas y reglamentos técnicos necesarios y, entre otras medidas, podrá emitir las relacionadas con el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica y de los servicios de almacenamiento tecnológico de documentos, o que el proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.

» CAPÍTULO IV: DE LOS SERVICIOS DE CERTIFICACIÓN

Requisitos generales.

Art. 43.- El servicio de certificación sólo podrá ser prestado por aquellas personas jurídicas, públicas o privadas, nacionales o extranjeras, que cumplan con los requisitos establecidos en las leyes competentes para operar en el país y que demuestren, para su autorización y durante todo el período en que se presten los servicios de certificación, cumplir con los siguientes requisitos:

a) Contar con suficiente capacidad técnica para garantizar la seguridad, la calidad y la fiabilidad de los certificados emitidos, de conformidad a los requerimientos contenidos en las normas técnicas.

b) Contar con el personal técnico adecuado, con conocimiento especializado comprobable en la materia y experiencia en el servicio a prestar.

c) Poseer la capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación. La capacidad antes mencionada, será medida no sólo por los equipos, insumos, licencias y otros bienes con los que cuente el proveedor de servicios de certificación para prestar sus servicios, sino también por el capital útil de trabajo con el que funcionará. Esta constatación la realizará la SIGET, a través de su Unidad de Firma Electrónica, mediante las auditorías y estudios

que considere conveniente y se revisará durante el tiempo de funcionamiento del proveedor.

d) Rendir fianza por un monto adecuado al riesgo asumido por la prestación de los servicios de certificación, el que se calculará conforme a los requerimientos definidos en el Reglamento de la presente Ley. Esta fianza será utilizada para indemnizar los daños y perjuicios que pudieren ocasionarse a los usuarios de los servicios de certificación. La fianza será revisada anualmente, tomando en cuenta los cambios en el nivel de riesgo asumido por el proveedor de servicios de certificación.

e) Contar con sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como a los certificados electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

f) Presentar el pliego tarifario de los servicios que se prestarán a los usuarios.

g) Satisfacer los demás requisitos previstos en esta Ley.

Acreditación de los Proveedores de Servicios de Certificación.

Art. 44.- Los Proveedores de Servicios de Certificación presentarán ante la Unidad de Firma Electrónica de SIGET, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo anterior. El cumplimiento de los requisitos será verificado por la Unidad de Firma Electrónica, a través de una auditoría inicial cuyo costo será sufragado por el solicitante.

En relación a las exigencias indicadas en las letras a) y b) del artículo anterior, el solicitante acreditará por escrito el compromiso de adquirir los equipos especializados necesarios y los servicios de personal técnico adecuado, en el plazo máximo que al efecto le indique la SIGET. Si transcurrido el plazo indicado el solicitante no hubiere cumplido el citado compromiso, se procederá inmediatamente a dejar sin efecto la acreditación otorgada.

El plazo de duración de la acreditación será por tiempo indefinido.

Equivalencia de certificados emitidos en el extranjero.

Art. 45.- Los certificados emitidos por prestadores de servicios de certificación de firma electrónica extranjeros, podrán ser reconocidos en los mismos términos y condiciones establecidos por esta Ley para los certificados nacionales, cuando cumplan una de las siguientes condiciones:

1) Si los certificados son reconocidos en virtud de acuerdo con otros países, ya sea bilaterales y multilaterales o efectuados en el marco de organizaciones internacionales de las que El Salvador forma parte.

2) Si los certificados son emitidos por prestadores de servicios de certificación debidamente avalados en su país de origen o instituciones homólogas a la Unidad de Firma Electrónica, que requieren para su reconocimiento estándares que garanticen la seguridad en la creación y regularidad del certificado, así como su validez y vigencia.

3) Se acredite que tales certificados fueron emitidos por un prestador de servicios de certificación que cumple con los estándares mínimos requeridos para un prestador de servicios de certificación de firmas electrónicas registradas en la Unidad de Firma Electrónica.

Los certificados electrónicos extranjeros que no cumplan las condiciones antes señaladas, carecerán de los efectos jurídicos que se atribuyen legalmente conforme a esta normativa; sin embargo, podrán constituir un elemento de convicción a valorar conforme a las reglas de la sana crítica.

Los certificados electrónicos emitidos por proveedores de servicios de certificación extranjeros, tendrán la misma validez y eficacia jurídica reconocida, siempre que cumplan con alguno de los requisitos antes mencionados.

Inicio de las actividades de Proveedores de Servicios de Certificación.

Art. 46.- El proveedor de servicios de certificación acreditado que inicie sus actividades, deberá dar notificación de este hecho a la Unidad de Firma Electrónica de SIGET, a más tardar diez días hábiles previos al inicio de tales actividades.

Obligación de Notificación.

Art. 47.- El cumplimiento de los requisitos exigidos por esta Ley para prestar los servicios de certificación, deberá asegurarse por todo el plazo en que el proveedor realice su actividad. Si surgen circunstancias dentro de las cuales esta garantía de cumplimiento ya no pueda ser mantenida, deberá notificarse de inmediato a la Unidad de Firma Electrónica.

Cuando se suscite cualquier modificación de la persona jurídica, incluyendo las relativas al control de la misma, deberá ser notificado oportunamente a la Unidad de Firma Electrónica.

Suspensión Temporal Voluntaria.

Art. 48.- El signatario podrá solicitar la suspensión temporal del servicio de certificación de la firma electrónica certificada, en cuyo caso su proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el signatario.

Obligaciones de los Proveedores.

Art. 49.- Los proveedores de servicios de certificación tendrán las siguientes obligaciones:

a) Adoptar las medidas necesarias para determinar la exactitud de los certificados electrónicos que proporcionen, la identidad y la calidad del signatario.

b) Garantizar la validez, vigencia, legalidad y seguridad del certificado electrónico que proporcione.

c) Garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas certificadas que proporcionen.

d) Verificar la información suministrada por el signatario.

e) Crear y mantener un archivo actualizado de certificados emitidos en medios electrónicos para su consulta por plazo indefinido.

f) Sin perjuicio de otras obligaciones establecidas en la Ley de Protección al Consumidor, deberá informar a los interesados de sus servicios de certificación, utilizando un lenguaje comprensible,

a través de su sitio de Internet y a través de cualquier otra forma de acceso público, los términos precisos y condiciones para el uso del certificado electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

g) Garantizar la autenticidad, integridad y confidencialidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo tecnológico confiable y seguro de dicha información.

h) Efectuar las notificaciones para informar a los signatarios y personas interesadas y las publicaciones necesarias acerca del vencimiento, revocación, suspensión o cancelación de los certificados electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con los mismos.

i) Dar aviso a la Fiscalía General de la República, cuando en el desarrollo de sus actividades tenga indicios de la comisión de un delito.

j) Cooperar con las autoridades del Ministerio Público y judiciales, cuando le sea requerido para la investigación de un delito o la presentación de una prueba.

k) Renovar anualmente la fianza establecida en el Art. 43, letra d), previo su vencimiento.

l) Cumplir con las demás obligaciones establecidas en esta Ley y su Reglamento.

El incumplimiento de cualquiera de los requisitos anteriores, dará lugar a las sanciones establecidas en la presente Ley.

Pérdida de capacidad tecnológica o económica de los proveedores de servicios de certificación.

Art. 50.- Cuando el proveedor de servicios de certificación pierda la capacidad técnica o económica necesaria para brindar el servicio posterior al inicio de sus actividades, determinado por auditoría o inspección, la SIGET determinará el plazo necesario para suplir dichas deficiencias.

En caso de no suplir dichas deficiencias, se aplicarán las sanciones previstas en esta Ley.

Responsabilidad por daños y perjuicios.

Art. 51.- Los proveedores de servicios de certificación serán responsables de los daños y perjuicios que ocasionen a sus usuarios, cuando deriven del incumplimiento de las obligaciones y requisitos establecidos en esta Ley y su Reglamento o del incumplimiento de sus obligaciones contractuales.

El proveedor de servicios de certificación también asume la obligación de resarcir por actos imputables a terceros, que hayan sido encargados por él para la realización de servicios en el cumplimiento de sus funciones.

Para la responsabilidad por daños y perjuicios, se observará el Código Civil; sin embargo, le corresponderá al proveedor de servicios de certificación probar la debida diligencia.

Notificación del cese de actividades.

Art. 52.- Cuando los proveedores de servicios de certificación decidan cesar en sus actividades, lo notificarán a la SIGET, al menos con noventa días de anticipación a la fecha de cesación.

La SIGET, después de haber recibido la notificación, emitirá una resolución dentro de los siguientes tres días hábiles, por medio de la cual se declare la cesación de actividades del proveedor de servicios de certificación como prestador de ese servicio, sin perjuicio de las investigaciones que pueda realizar, a fin de determinar las causas que originaron el cese de las actividades del proveedor y las medidas que fueren necesarias adoptar con el objeto de salvaguardar los derechos de los usuarios.

La SIGET ordenará al proveedor que realice los trámites necesarios para hacer del conocimiento de los usuarios y del público en general, la cesación de esas actividades y para garantizar la conservación de la información.

El proveedor de servicios de certificación trasladará sus usuarios activos a otro prestador, con la finalidad de garantizar la continuidad del servicio hasta la finalización del contrato, previo consentimiento expreso del usuario, sin que signifique costo adicional para éste último.

Si no existiere posibilidad de traspasar sus usuarios activos a otro proveedor, deberá notificar a los usuarios y a la SIGET, a través de la Unidad de Firma Electrónica, para que realicen las gestiones correspondientes para la extinción de los certificados. El procedimiento de compensación será regulado mediante el Reglamento de la presente Ley.

El proveedor de servicios de certificación deberá trasladar a SIGET la base de datos de los certificados en medio electrónico a que se refiere la letra e) del Art. 49 de la presente Ley.

En todo caso, el cese de las actividades de un proveedor de servicios de certificación conllevará la cancelación de su registro; sin perjuicio del pago de las obligaciones económicas pendientes derivadas de sus funciones.

» CAPÍTULO V: REGISTRO DE LOS PRESTADORES DE SERVICIOS DE ALMACENAMIENTO TECNOLÓGICO DE DOCUMENTOS ELECTRÓNICOS

Registro del prestador de servicios de almacenamiento tecnológico de documentos electrónicos.

Art. 53.- El servicio de almacenamiento tecnológico de documentos electrónicos sólo podrá ser prestado por aquellas personas jurídicas, públicas o privadas, que demuestren cumplir con los requisitos establecidos en el Art. 43 de esta Ley, tanto para su autorización, como durante todo el período en que se presten los servicios de almacenamiento tecnológico de documentos electrónicos.

Actividades de los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos.

Art. 54.- Los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, podrán realizar las siguientes actividades:

1. Ofrecer los servicios de procesamiento y almacenamiento tecnológico de documentos electrónicos.

2. Ofrecer los servicios de archivo y conservación de documentos almacenados tecnológicamente.

3. Cualquier otra actividad afín, relacionada con el almacenamiento tecnológico de documentos.

Obligaciones de los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos.

Art. 55.- Los prestadores de servicios de almacenamiento tecnológico de documentos electrónicos, tendrán las siguientes obligaciones:

1. Emplear personal calificado, con los conocimientos y experiencia necesarios para la prestación de los servicios de almacenamiento tecnológico de documentos electrónicos ofrecidos y los procedimientos de seguridad y de gestión adecuados.

2. Contar con sistemas confiables y productos que estén protegidos contra toda alteración y que garanticen un alto grado de seguridad técnica y de los procesos de almacenamiento tecnológico de documentos electrónicos que sirven de soporte.

3. Garantizar la protección, la confidencialidad y el debido uso de la información suministrada por el usuario del servicio.

4. Contar con un plan de contingencia que garantice la prestación continua de sus servicios.

5. Utilizar sistemas confiables para almacenar documentos electrónicos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos y se pueda detectar cualquier cambio que afecte a estas condiciones de seguridad.

6. Conservar el documento original por un período de diez años.

Cese de actividades.

Art. 56.- Todo prestador de servicios de almacenamiento tecnológico de documentos electrónicos que vaya a cesar en su actividad, deberá comunicarlo a la Unidad de Firma Electrónica de SIGET, siguiendo el procedimiento establecido en el Art. 52 de esta Ley.

Responsabilidad de los prestadores de servicios.

Art. 57.- El prestador de servicios de almacenamiento tecnológico de documentos electrónicos, responderá por los daños y perjuicios que ocasionen a los usuarios por el incumplimiento de las obligaciones que se establecen en esta Ley y su Reglamento, correspondiéndole al prestador del servicio demostrar que no ha incumplido ninguna de sus obligaciones.

El proveedor de servicios de almacenamiento también asume la obligación de resarcir por actos imputables a terceros, que hayan sido encargados por él para la realización de servicios en el cumplimiento de sus funciones.

Para la responsabilidad por daños y perjuicios, se observará el Código Civil; sin embargo, le corresponderá al proveedor de servicios de certificación probar la debida diligencia.

» CAPÍTULO VI: DE LOS CERTIFICADOS ELECTRÓNICOS

Garantía de la autoría de la firma electrónica certificada.

Art. 58.- El certificado electrónico garantiza la autoría de la firma electrónica certificada, así como la autenticidad, integridad, confidencialidad y no repudiación del documento electrónico.

Contenido del certificado electrónico.

Art. 59.- El certificado electrónico deberá contener, la siguiente información:

1. Identificación del titular del certificado electrónico, indicando su domicilio y dirección electrónica.

2. Identificación del proveedor de servicios de certificación que proporciona el certificado electrónico, indicando su domicilio y dirección electrónica.

3. Fecha de la acreditación y caducidad asignada al proveedor de servicios de certificación por la SIGET.

4. Fecha de emisión y expiración del certificado.

5. Número de serie o de identificación del certificado.

6. La firma electrónica certificada del prestador de servicios de certificación que emitió el certificado.

7. Datos de verificación de la firma, los cuales deben corresponder a la información de su creación y que están bajo el control del firmante.

8. Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el certificado electrónico.

9. Indicación de la ruta de certificación.

10. Si el certificado ha sido emitido por una persona que ha actuado en representación de una persona física o jurídica; en tal caso, el certificado deberá incluir una indicación del documento legal (público, privado o autenticado) que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona física o jurídica a la que represente.

La falta de alguno de estos requisitos invalidará el certificado.

Vigencia del Certificado Electrónico.

Art. 60.- El proveedor de servicios de certificación y el signatario, de mutuo acuerdo, determinarán el plazo de vigencia del certificado electrónico.

Cancelación del Certificado Electrónico.

Art. 61.- El certificado electrónico de la firma electrónica certificada puede ser cancelado por resolución judicial, de conformidad con el ordenamiento legal. Asimismo, puede ser cancelado por resolución razonada emitida por la SIGET, en cualquiera de los supuestos siguientes:

1. Que se compruebe que alguno de los datos del certificado electrónico proporcionado por el proveedor de servicios de certificación es falso.

2. Que sea violentado el sistema de seguridad del proveedor de servicios de certificación que afecte la integridad y confiabilidad del certificado.

3. Que el signatario dé aviso al proveedor de la destrucción o extravío del certificado electrónico. En tal caso, el proveedor de servicios de certificación procederá inmediatamente a la cancelación del certificado.

Procedimiento para la cancelación de un certificado electrónico.

Art. 62.- La SIGET, por medio de la Unidad de Firma Electrónica, previa denuncia del interesado o de oficio, ordenará audiencia por tres días hábiles al proveedor de servicios de certificación y con lo que conteste o no, se abrirá a pruebas por ocho días hábiles, a fin de demostrar cualquiera de las situaciones consideradas en el artículo anterior; finalizado el término probatorio, la SIGET emitirá resolución razonada, en un plazo no mayor de diez días hábiles para que determine si es procedente la cancelación del certificado que ampara la firma electrónica. Esta resolución admitirá

recurso de revisión y será resuelto en el plazo de quince días hábiles, con la vista de autos.

» CAPÍTULO VII: DE LOS DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE LOS SERVICIOS DE FIRMA ELECTRÓNICA CERTIFICADA Y CERTIFICACIÓN ELECTRÓNICOS

Derechos de los usuarios.

Art. 63.- Además de los derechos reconocidos por la Ley de Protección al Consumidor y cualquier otra normativa aplicable, los usuarios o titulares de los servicios regulados en esta Ley tendrán los siguientes derechos, según sea el caso:

1. A ser informados por los proveedores de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica certificada, así como de las reglas sobre prácticas de certificación y los demás que éstos se comprometan a seguir en la prestación de los servicios, lo que deberá realizarse de forma previa a la adquisición del servicio;

2. A la confidencialidad en la información, en los supuestos en que los proveedores de servicios de certificación y de almacenamiento tecnológico de documentos electrónicos decidan cesar en sus actividades;

3. A ser informados, antes de la emisión de un certificado, del pliego tarifario, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización de los servicios y de sus limitaciones de uso y de los procedimientos de reclamación y de resolución de litigios;

4 A que el prestador de servicios le proporcione la información sobre su domicilio en El Salvador;

5. A ser informado, al menos con noventa días de anticipación, por los prestadores de servicios de certificación y almacenamiento tecnológico de documentos electrónicos, para los efectos del cierre de actividades;

6. A traspasar sus datos a otro prestador de servicios de certificación y de almacenamiento tecnológico de documentos electrónico, si así lo solicitan.

7. A que el proveedor no proporcione u otorgue servicios no solicitados; deteriorar la calidad de los servicios contratados en calidad de inferioridad; o servicios adicionales cobrados no pactados; a no recibir publicidad comercial de ningún tipo por intermedio del proveedor, salvo autorización expresa del usuario en todos los casos señalados; y,

8. A que sean respetados los principios establecidos en el Art. 4 de esta Ley.

La violación a los derechos previstos en este artículo, constituye infracción grave en los términos señalados en la Ley de Protección al Consumidor y será sancionada como tal.

La determinación de la infracción y la imposición de la sanción correspondiente, será competencia del Tribunal Sancionador de la Defensoría del Consumidor y de acuerdo con el procedimiento previsto en la Ley de Protección al Consumidor, en lo que fuere aplicable.

Obligaciones de los usuarios.

Art. 64.- Los usuarios o titulares de firmas electrónicas certificadas y de almacenamiento tecnológico de documentos electrónicos quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a:

1. Brindar declaraciones veraces y completas.

2. Custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el prestador y actualizar sus datos en la medida que éstos vayan cambiando, so pena de responder por la indemnización de daños y perjuicios derivada del incumplimiento de estas obligaciones.

3. Solicitar oportunamente la suspensión o revocación del certificado, ante cualquier circunstancia que pueda haber comprometido la privacidad de los datos de creación de firma electrónica certificada.

TÍTULO IV: CAPÍTULO ÚNICO

» **DE LAS INFRACCIONES Y SANCIONES**

Infracciones aplicables a los proveedores de servicios de certificación y de almacenamiento tecnológico de documentos electrónicos.

Art. 65.- Los prestadores de servicios de certificación de firmas electrónicas certificadas y los Prestadores de Servicios de Almacenamiento Tecnológicos de documentos electrónicos, acreditados por la SIGET, están sujetos al régimen sancionador establecido en esta Ley.

Clasificación de las Infracciones

Art. 66.- Las infracciones de los prestadores, tanto de servicios de certificación de firmas electrónicas certificadas, como de servicio de almacenamiento tecnológico de documentos electrónicos, se clasificarán en leves, graves y muy graves.

1. Se consideran infracciones leves: El incumplimiento de las obligaciones señaladas en esta Ley y su Reglamento, cuando no hayan ocasionado perjuicios económicos a los usuarios de sus servicios o a terceros.

2. Se consideran infracciones graves:

a) El incumplimiento de alguna de las obligaciones establecidas en esta Ley y sus Reglamentos, cuando una resolución judicial establezca que se han ocasionado perjuicios económicos a los usuarios de sus servicios o a terceros, hasta doscientos cincuenta salarios mínimos de mayor cuantía.

b) La prestación de servicios sin realizar todas las declaraciones previas indicadas en esta Ley, en los casos en que no constituya una infracción muy grave.

c) El incumplimiento de los prestadores de servicios de las obligaciones establecidas para el cese de su actividad.

d) La resistencia, obstrucción, excusa o negativa injustificada a la inspección de la Unidad de Firma Electrónica de SIGET, así como la falta o deficiente presentación de la información solicitada por la misma, en su función de supervisión y control.

e) El incumplimiento de las resoluciones y reglamentos emitidos por la SIGET.

f) No suplir las deficiencias económicas o técnicas que motivaren las acciones previstas en el Art. 50 de la presente Ley.

g) No renovar las garantías exigidas con el objetivo de garantizar daños y perjuicios que pudieran ocasionarse a los usuarios de servicios de certificación y de almacenamiento tecnológico de documentos electrónicos.

h) Perder la capacidad para suspender, cancelar o revocar los certificados electrónicos que proporcione, según dictamen emitido por la SIGET.

i) Brindar información falsa, cuando sea solicitada por la SIGET.

j) Violar el secreto de la comunicación amparada con firma electrónica de sus usuarios.

k) Revelar información personal de sus clientes a terceros, sin el consentimiento expreso de éstos, salvo en los casos en que está obligado por ley. y,

l) El quebrantamiento de lo dispuesto en el Art. 5 sobre el tratamiento de datos personales.

3. Se consideran infracciones muy graves:

El incumplimiento de alguna de las obligaciones establecidas en esta Ley y sus reglamentos, cuando una sentencia judicial o administrativa establezca que se hayan causado perjuicios económicos a los usuarios o a terceros, superior a doscientos cincuenta salarios mínimos de mayor cuantía, o cuando la seguridad de los servicios que presta se hubiera visto gravemente afectada.

Sanciones.

Art. 67.- Por la comisión de las infracciones recogidas en el artículo anterior, SIGET impondrá las siguientes sanciones:

a) Por la comisión de infracciones leves, multa de 1 a 10 salarios mínimos de mayor cuantía.

b) Por la comisión de infracciones graves, multa de 11 a 500 salarios mínimos de mayor cuantía.

c) Por la comisión de infracciones muy graves, multa de 501 a 2500 salarios mínimos de mayor cuantía.

La reiteración en el plazo de dos años, de dos o más infracciones muy graves, sancionadas con carácter firme, dará lugar a la prohibición de la prestación de servicios de certificación de firmas electrónicas certificadas y de servicios de almacenamiento tecnológico de documentos electrónicos en la República de El Salvador.

La comisión de una infracción muy grave, una vez levantada la prohibición a que hace referencia este artículo, conllevará la cancelación definitiva de la prestación de servicios de certificación de firmas electrónicas.

Procedimiento y Recurso.

Art. 68.- Para la imposición de las sanciones por infracciones a la presente Ley, el Superintendente General de Electricidad y Telecomunicaciones ordenará la instrucción del expediente respectivo, mediante resolución razonada que contendrá la descripción de la conducta sancionable, la identificación del supuesto infractor y la relación de las pruebas con que se cuenta para determinar la correspondiente responsabilidad.

La resolución a la que se hace referencia en el inciso anterior, será notificada al supuesto infractor, quien deberá, dentro de los tres días siguientes a dicha notificación, expresar su inconformidad con los hechos atribuidos, presentando las pruebas de descargo que correspondan o solicitando la verificación de las mismas. Si el presunto infractor lo solicitara o la administración lo considerara necesario, se abrirá a pruebas el procedimiento por el término de ocho días. Transcurrido dicho plazo, se pronunciará la resolución que corresponda.

De la resolución que resuelva el proceso sancionador podrá ser interpuesto el recurso de apelación ante la Junta de Directores de la SIGET, en un plazo de cinco días hábiles, a partir del día siguiente a su notificación; debiéndose resolver el recurso en un término de diez días hábiles, agotándose la vía administrativa.

TÍTULO V: CAPÍTULO ÚNICO

» DISPOSICIONES FINALES

Reglamento y Normas Técnicas.

Art. 69.- El Presidente de la República deberá emitir el Reglamento de Aplicación de esta Ley.

Las normas y Reglamentos Técnicos que deba emitir la SIGET, lo serán en un plazo no mayor de seis meses.

Disposición transitoria.

Art. 70.- Cualquier persona natural o jurídica que al momento de entrar en vigencia la presente Ley se encuentre brindando servicios de certificación o almacenamiento tecnológico de documentos electrónicos, contará con un plazo no mayor a un año, para adecuarse al cumplimiento de los requerimientos establecidos por la misma, a fin de continuar brindando dicho servicio.

Disposiciones Supletorias.

Art. 71.- Las disposiciones y procedimientos contenidos en la Ley de Telecomunicaciones, podrán aplicarse, en lo que fuere pertinente.

Vigencia.

Art. 72.- El presente Decreto entrará en vigencia ocho días después de su publicación en el Diario Oficial.