USAID DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA | Programa Regional de USAID de Comercio para CAFTA-DR

Programa Regional de USAID de Comercio para CAFTA-DR

CUADRO DE RECOMENDACIONES A LAS MODIFICACIONES DEL ANTEPROYECTO DE LEY DE FIRMAS Y DOCUMENTOS ELECTRÓNICOS PARA EL SALVADOR.

Abril de 2010

Este documento ha sido elaborado por Alfredo Chirino para Chemonics International, Inc., para la revisión de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID).

INTRODUCCIÓN

El Programa Regional de USAID de Comercio para CAFTA-DR (CRT), en respuesta a la solicitud de la Secretaría Técnica de la Presidencia de El Salvador (STP), trabajó durante los años 2008 y 2009 en la elaboración de un anteproyecto de Ley de Comunicación y Firma Electrónica.

Este anteproyecto busca establecer el marco legal para otorgar plena validez y eficacia a la realización de transacciones a través de comunicaciones electrónicas, con o sin firma electrónica. Asimismo, busca regular la actividad de los proveedores de servicios de certificación.

La primera versión del anteproyecto fue hecha pública ante la sociedad civil a través de una serie de eventos en los cuales se explicó el alcance del anteproyecto y donde se recabaron los comentarios y sugerencias de las partes interesadas, con el fin de incorporarlos en una versión mejorada del anteproyecto. Esta versión fue finalizada y entregada a la STP en el 2009.

En abril de 2010, la STP solicitó asistencia adicional del CRT, con el fin de presentar un cuadro comparativo con las observaciones, sugerencias y cambios de redacción sugeridos para el proyecto de Ley de Firma Electrónica de El Salvador. Para este fin, el CRT contrató los servicios del consultor Alfredo Chirino, quien elaboró la versión final del anteproyecto incorporando las recomendaciones de la secretaría antes mencionada.

El cuadro comparativo de la Ley de Comunicación y Firma Electrónica, producto de esta consultoría, se incluye a continuación en este informe.

CUADRO DE CAMBIOS A PARTIR DE LA CONSULTORÍA DE ABRIL DE 2010 (EL SALVADOR) LEY DE COMUNICACIÓN Y FIRMA ELECTRÓNICA[1]

PROYECTO DE LEY ACTUAL	CAMBIOS SUGERIDOS	JUSTIFICACIÓN	COMENTARIOS
I.- Que la Constitución de la República en el Art. 101 inc. 2 establece que el Estado debe promover el desarrollo económico y social mediante el incremento de la producción, productividad y racionalización de los recursos, en consecuencia, debe ofrecer los instrumentos legales que propicien las innovaciones tecnológicas que brinden oportunidad para el acceso a la información en ciencias, educación o en la realización competitiva de transacciones.	**I**.- Que la Constitución de la República de El Salvador, Art. 101, inciso 2, 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 ofrecer los instrumentos legales que propicien innovaciones tecnológicas que brinden oportunidad para el acceso a la información en ciencias, educación, o en la realización competitiva de transacciones. De igual manera, debe el Estado garantizar que los ciudadanos y ciudadanas tengan una adecuada protección jurídica en sus interacciones en nuevos mercados, y en entornos tecnológicos novedosos, de tal manera que sus derechos como consumidores no sean menoscabados.	**No sólo debe promoverse el acceso a nuevos medios de desarrollo económico y promover la utilización de recursos y crear condiciones de nuevos medios de comercio, sino que también debe protegerse al ciudadano en su condición de consumidor, sobre todo en nuevos entornos de mercado, transfronteras.**	**La propuesta fue sugerida por los expertos de CONAMYPE.**
II.- Que la Constitución de la República en el Art. 2 reconoce que toda persona tiene el derecho a la seguridad jurídica, por lo que el Estado debe brindar seguridad en las comunicaciones electrónicas y las transacciones autorizadas mediante las aplicaciones de la tecnología o la suscripción electrónica de las mismas, tengan validez jurídica; y,			**En relación al "Considerando II" del Proyecto de Ley, los expertos de CONAMYPE indicaron que debía trabajarse efectivamente en un marco legal que realmente brindara seguridad jurídica y por ello establecer el proyecto de ley los cánones en que esta seguridad jurídica será garantizada, así como también los delitos informáticos implícitos. Sin embargo, dicha tarea no corresponde a una ley de firma y mensajes electrónicos, se requiere reformas al Código Penal que permitan este adelantamiento de la defensa del ciudadano y, por supuesto, cambios en otras leyes especiales, como lo sería por ejemplo el Código Civil y de Comercio.**

III.- Que la Sociedad de la Información se ha convertido en un factor estratégico que mejora la eficiencia de la educación y fomenta la competitividad y el crecimiento económico de los pueblos y asimismo, eleva la calidad de vida de los ciudadanos, razón por la cual nuestro país por medio de esta ley se integra al entorno mundial de comunicaciones electrónicas;	**III.-** Que el desarrollo de las modernas tecnologías de la información y de la comunicación se ha convertido en un factor estratégico que mejora la eficiencia de la educación y fomenta la competitividad y el crecimiento económico de los pueblos y asimismo, eleva la calidad de vida de los ciudadanos, razón por la cual nuestro país por medio de esta ley promociona un uso inteligente de estas tecnologías para propiciar el comercio y el desarrollo económico, incorporando al país al entorno mundial en que se producen interacciones seguras en materia de comercio electrónico;	**CONAMYPE sugirió cambiar el punto de partida de la "sociedad de la información", indicando que es un término más propio de las ciencias informáticas y que era necesario hacer cambios en el considerando.**	**Se ha cambiado el "considerando III" para motivar el cambio producido por la ley a partir del desarrollo vertiginoso de las tecnologías de la información y de la comunicación, de las que El Salvador es partícipe y no excepción. A partir de allí se ubica el trabajo del legislador como parte de una preocupación por insertar al país en el comercio electrónico mundial, donde se requiere seguridad.**
Objeto Art. 1.- La presente ley tiene por objeto brindar seguridad jurídica a los usuarios de las tecnologías de información y comunicación cuando realicen transacciones a través de comunicaciones electrónicas con o sin firma electrónica con la finalidad de que se otorgue plena validez y eficacia jurídica a las transacciones así realizadas.	**Objeto** Artículo 1. La presente ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.	**CONAMYPE insiste en un posible sinsentido jurídico del reconocimiento de comunicaciones electrónicas con o sin firma electrónica. Dice que si se está reconociendo también el valor jurídico de comunicaciones sin firma, no tendría sentido regular todo el tema de las firmas electrónicas proveídas por los prestadores de estos servicios.**	**Tienen razón los expertos de CONAMYPE: la redacción del proyecto, con los cambios hechos por la comisión salvadoreña, podrían provocar un sinsentido jurídico, sería mejor acudir al tenor literal original que la ley tiende a regular la firma electrónica, el mensaje de datos y a las informaciones inteligibles, sin importar su formato o soporte, y decir que también regula el trabajo de los proveedores de servicios de certificación. De esa manera se cierra, adecuadamente la orientación del proyecto y se fijan los principales objetivos normativos del proyecto. Además, debe tenerse en cuenta que las transacciones son solo una parte de las comunicaciones electrónicas, también los correos electrónicos y otras formas de mensajes de datos merecen análisis legislativo.**

Interpretación progresiva Art. 2.- Las regulaciones de la presente ley serán aplicables a la comunicación electrónica, firma electrónica 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 los principios de autenticidad, integridad, confidencialidad, equivalencia y no repudiación a fin de reconocer la validez y eficacia probatoria de los mensajes de datos y firma electrónica conforme a esta ley.			**La sugerencia del BMI es de recibo y se acoge.**
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 a los proveedores de servicios de certificación para operar y proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidas en la presente ley; **Certificado Electrónico:** Documento proporcionado por un proveedor de servicios de certificación que verifica la correspondencia entre la clave pública y clave privada con su titular, otorgándole certeza y validez a la firma electrónica;		**El BMI indica que el concepto de "firma electrónica" que establece el Art. 3, debe reflejar que es el equiparable al otorgamiento del consentimiento libre y expreso de su titular en un acto o negocio determinado. No solo limitar a la voluntad de firmar. La observación tiene razón en dos aspectos: por una parte la definición consignada en el proyecto tiene que ver directamente con el problema de la tecnología de clave pública/clave privada que es el estándar internacional, pero que para nada debe convertirse en el único y, por otra parte, se queda en la expresión de la voluntad de firmar.**	**En efecto, se trataría de una relación de género a especie, ya que la firma "digital" no es más que una forma de firma electrónica, por lo que no habría necesidad de considerarla por aparte.**

Clave privada: Es la clave generada por un proceso matemático que contiene datos únicos que el firmante utiliza para crear la firma electrónica. Su conocimiento y control es exclusivo del firmante **Clave pública:** Es aquella clave generada por un proceso matemático que contiene datos únicos que permiten verificar la firma electrónica del firmante. Su conocimiento es público; **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, el telegrama, el télex o el telefax; **Firma Electrónica**: Es la combinación de clave pública y privada que asocia a una persona con su voluntad de firmar, utilizando sistemas criptográficos asimétricos, contenida en un certificado expedido por un proveedor de servicios de certificación acreditado; y, **Proveedor de Servicios de Certificación:** Persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en esta ley.	Se sugiere la siguiente redacción del concepto de firma electrónica en el artículo 3: **"Firma Electrónica"**: se entenderá por este concepto los datos en forma electrónica consignados en un mensaje de datos, o adjuntados 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."	**El Banco Central de Reserva indica que el proyecto no contiene una definición de "firma digital" y en ese sentido se consideraría un sinónimo.**	
Art. 4.- Las actividades reguladas por esta ley se regirán bajo los siguientes Principios: **a) Autenticidad[2],** con la cual se garantiza que el mensaje es confiable y ésta garantía perdura a través del tiempo.	Se debe incluir un literal f) en el art. 4 que dirá: f) Por "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,	**En los literales "c" y "e" de este artículo se utiliza el término iniciador, el cual no ha sido incluido en el apartado sobre definiciones de la ley.** **Como referencia se puede utilizar la siguiente definición:** **Por "iniciador" de un mensaje de datos se**	**Sugiere el Banco Central de la Reserva volver al concepto de "iniciador" que viene en la ley de CNUDMI, es una buena idea que busca claridad en un concepto importante para esta ley y para el tema del comercio electrónico.**

b) Integridad, por medio del cual se otorga certeza de que los datos recibidos por medios electrónicos no han sido modificados en su tránsito desde el iniciador hasta el destinatario **c) Confidencialidad**, por medio de la cual se garantiza al iniciador y destinatario que los mensajes electrónicos no serán conocidos por terceras personas sin su expresa autorización. **d) Equivalencia**, a través del cual no puede negarse la presentación de documentos electrónicos en instancias administrativas o judiciales, solo por encontrarse contenido en un soporte diferente al físico. **e) No Repudiación**, por medio del cual se garantiza que cuando un mensaje ha sido suscrito con firma electrónica de conformidad a lo establecido en la presente ley, no puede ser repudiada su autoría por la persona del iniciador.	si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él.	**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;** **CONAMYPE manifiesta inquietud acerca del principio de equivalencia, pero sobre todo por la eventual posibilidad de admitir documentos que no cumplen los requisitos de ley, sobre todo los requisitos ad solemnitatem que están previstos en la ley para brindar legalidad y seguridad jurídica. Por ello, recomiendan que dicha redacción debe aceptar que si no llena los requisitos de ley tanto para su emisión como los requeridos por las leyes para validarlos debe resolverse su inadmisión, tal como sucede con los que se presentan en el ámbito físico.**	**En realidad, esta definición de equivalencia alude a un principio general, no es una disposición ordenatoria o regulatoria. El principio de equivalencia exige que no se haga diferencia en la legislación entre documentos solo porque algunos están en formato electrónico. Distinto es el valor jurídico que se le dará a estos documentos, que eso es materia de los Códigos Procesales y de esta ley que entra en el tema más adelante.**
Tratamiento de datos Art. 5.- El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad se sujetará a las siguientes reglas: a) Para la expedición de certificados electrónicos al público, los	**Tratamiento de datos personales**	**Resulta conveniente hacer referencia a que el artículo 5 se refiere al tratamiento de datos personales por parte de los servicios de firma y certificación electrónicas.**	**Esta sugerencia es correcta y coincide con el sentido jurídico de la regulación. En ella coinciden CONAMYPE y el Banco Central de la Reserva de El Salvador.**

prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos. Toda cesión de datos personales también requerirá el consentimiento expreso de su titular, quien podrá solicitar la rectificación o cancelación de los datos personales cuando tales datos sean contrarios a lo previsto en este capítulo o cuando fueren inexactos o incompletos; b) Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante; c) Los proveedores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo solicite el juez competente o 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 al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el responsable del registro de datos.		**CONAMYPE sugiere que deben cerrase la brechas para los contratos de adhesión, por lo que se recomienda la redacción siguiente: "b) Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico"** **CONAMYPE sugiere que siempre debe agregarse que estos mensajes de datos deben cumplir los requisitos legales que las leyes de la materia establezcan so pena de nulidad.**	**El sentido de una regulación de protección de datos personales es procurar, en primera instancia que los datos sean tratados únicamente para los fines para los que fueron recogidos. Cualquier cambio a este uso tendría que realizarse sólo con el consentimiento del usuario. Por ello no puede evitarse los contratos de adhesión por esta vía.** **No puede accederse al cambio sugerido ya que la regulación de requisitos legales de formalidad (ad solemnitatem) no serán cambiados por esta ley y seguirán existiendo a pesar de que el documento en concreto se manifieste en forma electrónica.**

Equivalencia jurídica Art. 6.- El mensaje de datos utilizando firma electrónica cualquiera sea su medio de transmisión o de almacenamiento, se tendrá por jurídicamente equivalente al contenido en documentos convencionales que se otorguen, almacenen o se transmitan por medios físicos.			
Celebración por escrito Art. 7.- En todos los casos en que se exija que una información conste por escrito o deba ser presentada en esa forma o se prevean consecuencias jurídicas si la información no consta por escrito, se entenderá que un documento contenido en un soporte electrónico, cumple con el requisito de escrituralidad, siempre y cuando la información cumpla con los principios y requisitos exigidos por esta ley. No obstante lo anterior, el empleo del soporte electrónico para un documento determinado no dispensa en ningún caso el cumplimiento de los requisitos, formalidades o solemnidades que el ordenamiento legal exige para cada acto jurídico en particular.	En lugar de “escrituralidad” debe usarse “forma por escrito”	**CONAMYPE sugiere que el documento puede cumplir con el requisito de escrituralidad, pero también debe cumplir con las formalidades que las leyes exigen para que tenga validez, por lo que debe cumplir con las solemnidades establecidas ya que de lo contrario se estaría fomentando la inseguridad jurídica. Ej. un matrimonio no puede celebrarse solo con la comparecencia de los contrayentes. No debe olvidarse los vicios del consentimiento y las nulidades por falta de cumplimiento de formalidades. Por lo que este proyecto requiere previamente se legisle sobre que actos o contratos puede utilizarse. También es de aclarar que todos lo actos de la Administración Publica pueden comprenderse de esa forma ya que los actos que realizan los funcionarios públicos solo son validos si son realizados de conformidad con la Ley. caso contrario son nulos.**	**Tampoco puede accederse a este cambio ya que casualmente el artículo 7 tiende a mantener los requisitos ad solemnitatem y ad probationem que la ley contempla. Si algún documento o acto jurídico requiere solemnidades específicas para surtir efectos jurídicos ante terceros o para servir de prueba, sólo lo hará en la medida que cumpla tales requisitos. El documento electrónico habrá de cumplir en todos los casos las formalidades y solemnidades contempladas en la ley. Habrá actos que no podrán realizarse vía documento electrónico, como es el caso del matrimonio, por ejemplo. El Banco Central de la Reserva sugiere revisar el uso idiomático de la palabra “escrituralidad” que no parece ser un giro aceptado en diccionarios generales o especializados. Es conveniente cambiar “escrituralidad” por “forma por escrito.**

Exigencia de documento original Art. 8.- Si de acuerdo al acto jurídico o por disposiciones del ordenamiento legal se exija que la información sea conservada en su forma original, se entenderá que un documento electrónico cumple dicha exigencia si la firma electrónica demuestra que no ha sido alterado, el cual puede ser presentado en soporte diferente en caso de destrucción del soporte electrónico.		**CONAMYPE sugiere que este aforismo desvincula el principio de seguridad que inclusive esta amparado en los documentos físicos, si un documento es destruido no puede ninguna copia hacerse valer como original, ya que de aceptarse esto se estaría dando a un mismo documento acción ilimitada y valdría su acción tantas veces como el poseedor quiera demandar. El principio de que nadie puede ser condenado dos veces por la misma causa se rompe.**	**El artículo no hace referencia a lo que CONAMYPE sugiere, sino que más bien traslada el principio de equivalencia a la exigencia, en algunos casos, de que el documento electrónico (que no tiene contraparte de papel, por ejemplo) pudiera exigirse en su formato original (que sin duda será electrónico: un correo electrónico, por ejemplo) y a partir de allí, ya sea por razones judiciales o de la propia negociación, se solicite que sea presentado el original, en tal caso se dice que se entenderá que es tal, es decir, el original, si la firma electrónica de fe de que no ha sido alterado. Esto último puede alcanzarse con la tecnología disponible de certificación digital.**
Conservación de documentos Art. 9.- Si la ley exige que los documentos, registros, datos o información pública o privada sean conservados en archivos, se entenderá que cumple con dicha exigencia cuando permita mantener su autenticidad, integridad, confidencialidad, equivalencia, no repudiación y otros que la ley o el reglamento establezcan.	Se sugiere la siguiente redacción: **Constancia por escrito del mensaje de datos**[4] Artículo 9.- Si la ley requiere que la información contenida en un mensaje de datos conste por escrito, tal 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 su soporte permanezca accesible, conservado o archivado por un periodo determinado de tiempo o en forma permanente, esto se podrá cumplir mediante un mensaje de datos, si este cumple con los siguientes requisitos: 1. Que la información que contenga pueda ser consultada posteriormente. 2. Que conserven el formato que se generó, archivó o recibió o en algún	**CONAMYPE parte de que el artículo 9 se refiere a la conservación de originales físicos, y sugiere que en tal caso debe dejarse claro que si un documento original físico entra en contradicción con el magnético debe quedar claro que prevalece el físico sobre el electrónico.**	**La inquietud de CONAMYPE es de recibo ya que con la redacción actual del proyecto se estaría aludiendo a una conservación por escrito de documentos electrónicos, cuando la orientación original del Anteproyecto era sobre la exigencia legal de los mensajes de datos por escrito. A esto se refieren las reglas, así como los requisitos que contenía originalmente sobre la forma en que podía establecerse este requisito y el papel eventual de un tercero en la prestación de los servicios.**

	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. Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados por este artículo.		
Documentos auténticos y públicos emitidos en soportes electrónicos[3] Art. 10.- Los documentos auténticos podrán estar contenidos en soporte electrónico y tendrán el valor asignado por el ordenamiento legal para esta clase de documentos. Los documentos públicos electrónicos que se refieran al ejercicio de la función notarial se regularán en una ley especial[1].		**CONAMYPE menciona en relación a este artículo 10 que habría que esclarecerse a qué documentos auténticos y públicos se está refiriendo la ley de firma electrónica, ya que la gama de instrumentos que se conocen como públicos y que solo se pueden hacer valer con la presentación física.**	**El artículo 10 está haciendo referencia a la eventual digitalización de documentos auténticos, así como documentos auténticos que pudieran estar conservados en formato electrónico. El artículo les da el mismo valor que los documentos auténticos y públicos disponibles en formato manual. A párrafo seguido resuelve conceder un régimen especial a los documentos públicos electrónicos que pudieran emanar de la función notarial. El listado que sugiere CONAMYPE, podría ser siempre incompleto y llevaría a posibles dificultades para la actualización de la ley. Es mejor dejar la regla general del artículo 10.**

1

Valor Probatorio de los documentos privados electrónicos Art. 11.- Cuando el documento privado fuera generado con firma electrónica y se refiera a actos jurídicos que no se encuentren excluidos por la presente ley, el valor del mismo será de plena prueba y tendrá fuerza ejecutiva en su caso, sin embargo, no podrá presentarse para su cobro más de una vez.		**Menciona CONAMYPE que de conformidad a la legislación salvadoreña, los documentos privados no tienen fuerza ejecutiva, esto vendría al traste con toda nuestra legislación, no se le puede dar el carácter de publico a un documento privado este debe ser sometido a su reconocimiento por la vía judicial. la ley ya establece cuales son considerados documentos con fuerza ejecutiva.**	
Verificación de la emisión del Mensaje de Datos Art.12.- 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 el documento ha sido firmado electrónicamente. b) Por un sistema de información programado por el iniciador, o bajo su autorización, para que opere automáticamente.		**Según CONAMYPE la figura del mandato esta regulada en la legislación salvadoreña y tiene anejas solemnidades para cada caso en concreto, el regularlo de esta forma sin considerar dichas previsiones normativas generaría imposibilidades jurídicas y conflictos de carácter procesal.**	**En general, el artículo 12 no se refiere al mandato, más allá de la posibilidad de que haya un poder conforme a la legislación salvadoreña que faculte a una persona física o jurídica convertirse en iniciador de un mensaje y enviarlo electrónicamente, añadiéndole, por supuesto, una firma electrónica.**
Reglas para la determinación del recibo del mensaje. Art. 13.- El recibo del mensaje, se comprobará por el sistema de la recepción y tendrá lugar cuando el mensaje de datos ingrese al repositorio destinatario, encontrándose a disposición de éste para su acceso. Las partes no podrán pactar lo contrario a esta disposición.		**Sugiere CONAMYPE que se revise la teoría del domicilio vigente en el país**.	**Las reglas del domicilio no son de recibo acá, sino las que las partes definan para la relación contractual que las une. Acá están siendo aplicadas las IAREDS de la OEA en materia de firma electrónica y comercio electrónico.**

Lugar de emisión y recepción Art. 14.- Salvo prueba en contrario, el mensaje de datos se tendrá por emitido en el lugar donde el iniciador tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo. Prevalecerá el domicilio establecido por las partes; 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.		**Solicita CONAMYPE se tengan en cuenta aquí las sugerencias sobre lo expresado revisar lo dicho sobre el lugar de emisión y recepción.**	**Aplican los comentarios hechos sobre el tema del domicilio y los criterios expresados sobre las reglas de emisión.**
Del acuse de recibo Art. 15.- Los usuarios podrán acordar los mecanismos y métodos para el acuse de recibo de un mensaje de datos. Cuando los usuarios no hayan acordado que para el acuse de recibo se utilice un método determinado, se considerará que dicho requisito se ha cumplido cuando: a) La comunicación dirigida al destinatario permita corroborar la recepción del mensaje de datos. b) A través de actos del destinatario, el iniciador pueda evidenciar que ha recibido su mensaje de datos.		**Dice CONACYPE que en El Salvador no se cuenta con una ley de documento único electrónico, por lo tanto la firma electrónica tendría el inconveniente de identificación legal de las personas.**	**En realidad, no se entiende el comentario de CONACYPE, ya que la identificación de las personas no depende de un tema legal sino de las tecnologías que respaldan la emisión de la firma y del certificado digital que contienen.**
Requisitos y efectos de la firma electrónica Art. 16.- La firma electrónica debe estar sustentada en un método de creación y verificación confiable y seguro, de manera que aquella sea inalterable, alertando al destinatario en caso de alteración de la información después de ser suscrita por el signatario. La firma electrónica tiene los siguientes efectos:		**CONACYPE indica que debe aclararse que un documento privado y tendrá la validez que estos documentos tengan según la legislación aplicable. (civil, mercantil)**	**La aclaración no es indispensable, ya que el artículo 17 parte de los efectos jurídicos que la ley le dé a la firma manuscrita a partir del principio de equivalencia para la firma electrónica, no se le da entonces un efecto jurídico distinto a la firma electrónica. Esto en plena concordancia con todo el régimen jurídico preestablecido en el Anteproyecto.**

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. 17.- La firma electrónica 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 realidad, nadie ha afirmado que a través de una firma electrónica no se pueda avalar una falsedad, lo que sucede es que la tecnología permite garantizar el contenido (integridad) e identidad del emisor, pero eso no significa que se garantiza un negocio lícito. La firma electrónica puede ser utilizada para cometer delitos y defraudaciones, eso es algo inevitable porque depende del dolo y malas intenciones de quienes la utilizan. Ninguna ley evitará o prevendrá que esto ocurra.**
Presunciones del empleo de la firma electrónica Art. 18.- El empleo de la firma electrónica que cumpla los requisitos exigidos en la presente ley, salvo prueba en contrario, presume lo siguiente: a) Que la firma electrónica pertenece al titular de la misma; b) Que el mensaje de datos vinculado a la firma electrónica no ha sido modificado desde el momento de su envío, si el resultado del procedimiento de verificación así lo indica.		**CONACYPE menciona que este artículo 18 reconoce, prácticamente, que puede haber falsedad en el mensaje o la firma electrónica.**	**En general, el sistema de firma electrónica debe servir para favorecer los servicios de valor agregado que ofrece el Estado dentro de su plan de gobierno electrónico. El CAUCA IV y el RECAUCA IV, incluso, ya prevén el uso de la firma electrónica para los servicios aduaneros. Se vislumbra también el uso de firma electrónica para impuestos, para la interacción con oficinas estatales, para el manejo de expedientes judiciales y administrativos en forma electrónica. Impedir que la administración use la firma electrónica es limitar uno de los usos más importantes que esta tiene en cualquier país moderno.**

Uso de la firma electrónica por representantes Art. 19.- Podrán hacer uso de la firma electrónica, los representantes legales de las personas jurídicas públicas o privadas y en tal caso, el certificado electrónico deberá contener los datos necesarios para la identificación de la persona jurídica y de su representante legal. Para los mandatarios de las personas naturales, solo se utilizará la firma electrónica de aquel, previa verificación de tal calidad por parte del proveedor de servicios de certificación, ésta circunstancia deberá constar en el certificado que se le extienda. No podrán hacer uso de firma electrónica los padres por sus hijos ni los tutores o curadores por sus pupilos.		**Sugerencia del BMI para evitar repetición en el art. 20.** **CONACYPE insiste en relación con el artículo 19 que la ley debería de dejar la aplicación de la ley de firma electrónica, únicamente a las entidades privadas ya que en El Salvador, la legislación, considera que la función publica esta claramente reglamentada y traería consecuencias graves el permitir que los funcionario públicos utilicen los medios electrónicos para comunicar las resoluciones o ejecuten actos que requieren un proceso de autorización y al no cumplirlos son nulos y no son reconocidos por el Estado, quedando a los particulares únicamente el derecho de demandarlos.**	**CONAMYPE insiste en el no uso de la firma electrónica en el sector público, un área donde sin duda tendrá efectos positivos para el país. No hay necesidad de cambios constitucionales para implementar y ejecutar la ley de firma electrónica.**
Prestación de servicios públicos mediante mensaje de datos y firma electrónica Art. 20.- Los funcionarios y empleados públicos que presten servicios públicos, ejecuten o realicen actos o expidan cualquier documento, dentro de su ámbito de competencia, podrán suscribirlos por medio de una firma electrónica. El proveedor de servicios de certificación deberá consignar en el certificado la calidad con la que firmará electrónicamente. Se exceptúan del uso de la firma electrónica, en aquellas actuaciones para las cuales la Constitución de la República o la ley exijan alguna solemnidad que no sea susceptible de cumplirse mediante documentos electrónicos, mensaje de datos o firmas electrónicas, o requiera la concurrencia personal de la autoridad pública que deba intervenir en ellas.	Se sugiere un cambio en la redacción del artículo 20 para evitar repeticiones: “Prestación de Servicios Públicos mediante mensaje de datos y firma electrónica Art. 20.- Los funcionarios y empleados del Estado que presten…	**Insiste CONAMYPE que mientras no se reformen las leyes que rigen al Estado y se modifique la Constitución no es recomendable que los funcionarios extiendan documentos a través de este sistema, lo que si se puede implementar es la comunicación oficial entre entidades ocupando este tipo de mecanismo no como documentos auténticos o públicos sino como simple copia de comunicación.**	**Hay que insistir que los funcionarios públicos, en la medida que puedan emitir documentos auténticos podrán emitirlos en forma electrónica mediante una firma certificada, dicho proceso proviene de la autorización genérica que el principio de equivalencia ya habilita para todo el ordenamiento jurídico. Por supuesto, habrá actos solemnes que seguirán teniendo firma escrita hológrafa en la medida que el ordenamiento jurídico lo exija así.**

Validez de actos y contratos Art. 21.- Los actos y documentos de las Instituciones del Estado que tengan la calidad de instrumento auténtico, podrán suscribirse mediante firma electrónica.		**También en cuanto al artículo 21 CONAMYPE continúa en su escepticismo en cuanto al uso de la firma electrónica en el sector público.**	
Interacción electrónica entre administrados y funcionarios públicos Art. 22.- Las personas podrán relacionarse con las Instituciones del Estado, sin necesidad de firma electrónica, siempre que se ajusten a las técnicas y medios electrónicos establecidos para tal fin. El uso de la firma electrónica del particular en la interacción con el Estado solo será necesario en casos de suscripción de contratos o cuando la ley expresamente exija firma.		**Insiste CONAMYPE que de igual forma los contratos celebrados con el Estado están dotados de solemnidades que no se pueden omitir. La firma es de carácter obligatoria en la suscripción de contratos con el estado de igual forma la identificación fehaciente de la persona tanto natural como jurídica.**	
Conservación, registro y archivo Art. 23.- 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, sin embargo, no podrán destruirse los documentos originales sin la previa verificación y colaboración del Director del Archivo General de la Nación.			
Comunicaciones electrónicas Art. 24.- Cualquier Institución del Estado, siempre y cuando cuente con la infraestructura tecnológica adecuada podrá practicar comunicaciones por vía electrónica, utilizando firma electrónica, tales como citaciones y notificaciones, siempre y cuando el destinatario de los servicios públicos		**En el caso de la aplicación del art. 24 al Poder Judicial, indica CONAMYPE que es preciso especificar que las notificaciones deben ser personales y la CSJ ha sido clara en sus Sentencias, en lo que respecta a esta circunstancia. Se recomienda que se consulte a dicho Órgano del Estado.**	**Es razonable la sugerencia que hace CONAMYPE, la que fue ratificada en los foros de discusión organizados por el Ministerio de Economía. El Poder Judicial debería de ser una de los órganos del Estado que debería de ser consultado en este caso. No obstante, las objeciones**

hubiera autorizado ese medio de comunicación. Dicha autorización surtirá efecto mientras el destinatario no comunique una modificación al respecto.			**hechas a la notificación electrónica no parecen ser sustentables tomando en cuenta experiencias similares, como la de Costa Rica que las hace, incluso sin firma electrónica.**
La Autoridad de Control y Vigilancia Art. 25.- La Superintendencia General de Electricidad y Telecomunicaciones por medio de la Gerencia de Acreditación de Servicios de Certificación será competente para la acreditación, control y vigilancia de los proveedores de los servicios de certificación electrónica de conformidad con esta ley y su reglamento, sin perjuicio de las competencias que esta ley confiere a la Defensoría del Consumidor o a alguno de sus órganos. **De la Gerencia de Acreditación de Servicios de Certificación** Art. 26.- La SIGET organizará la Gerencia de Acreditación de Servicios de Certificación quien estará a cargo de uno de sus funcionarios, el cual será nombrado por el Superintendente.	Se sugiere cambiar el orden de los artículos 25 y 26 del Proyecto, y la redacción del artículo 25, para que se lean así: **La Autoridad de Control y Vigilancia** Art. 25.- Crease la Gerencia de Acreditación de Servicios de Certificación Electrónica y Firma Electrónica como una unidad de la Superintendencia General de Electricidad y Telecomunicaciones (SIGET). Uno de los funcionarios de SIGET estará a cargo de esta Gerencia y su designación será realizada por el Superintendente. **De La Gerencia de Acreditación de Servicios de Certificación.** Art. 26.- La Superintendencia General de Electricidad y Telecomunicaciones por medio de la Gerencia de Acreditación de Servicios de Certificación será competente para la acreditación, control y vigilancia de los proveedores de los servicios de certificación electrónica de conformidad con esta ley y su reglamento, sin perjuicio de las competencias que esta ley confiere a la Defensoría del Consumidor o a alguno de sus órganos.	**CONAMYPE, con relación al artículo 25, indica que es de recalcar que en la ley se debe establecer con claridad todos los requisitos que deberán cumplir los proveedores de los servicios de Acreditación Electrónica, y no pensar que se desarrollarán en el reglamento, ya que en el reglamento no se pueden establecer requisitos u obligaciones que no estén estipuladas en la Ley**. **En cuanto al orden del articulado de la Ley, la Superintendencia de Valores sugiere un cambio en el orden de los diversos numerales del 25 y 26 proponiendo que el artículo 25 se refiera a la creación de la Gerencia de Acreditación y luego el 26 con la definición de la competencia.** **En cuanto al Artículo 26, sugiere CONAMYPE que diga en adelante: "Art. 26 Crease la Gerencia de Acreditación de Servicios de Certificación Electrónica y Firma electrónica como una unidad de la Superintendencia General de Electricidad y Telecomunicaciones.**	**Lo que dice CONAMYPE ha sido tomado en cuenta en el Anteproyecto de Ley, y es uno de los elementos que fueron incluidos desde sus versiones iniciales y está consignado en el artículo 32 de la Ley que establece los requisitos de los proveedores de firma electrónica y certificados digitales.** **La recomendación es aceptada. El cambio de orden de los aspectos regulados le da más claridad a la exposición de la ley.** **El artículo 26 (que se sugiere que ahora sea artículo 25) solo dice que se "organizará" por parte de SIGET una Gerencia de Acreditación, pero lo preferible es, y en esto lleva razón CONAMYPE, que la mencionada Gerencia sea creada por ley y que sea por esta que alcance su competencia funcional.** **Aun cuando pudiera sentirse como una repetición, puede dar más claridad al sentido último del proyecto, en cuanto a que el Gerente designado habrá de cumplir también los requisitos legales establecidos en la Ley de SIGET.**

Requisitos del Gerente de Acreditación de Servicios de Certificación Art. 27.- El Gerente de Acreditación de Servicios de Certificación deberá reunir los requisitos exigidos en la Ley de Creación de la Superintendencia General de Electricidad y Telecomunicaciones para los gerentes de la Institución.		**CONAMYPE sugiere que este artículo 27 es innecesario, ya que no aporta algo distinto a lo ya contemplado en la Ley de SIGET.**	
" "Competencias de la SIGET para la aplicación de la presente ley Art. 28.- La SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación, tendrá las siguientes competencias: 1. Otorgar la acreditación a los proveedores de servicios de certificación una vez cumplidas las formalidades y requisitos de esta ley, su reglamento y demás normas técnicas aplicables. 2. Validar los certificados de los diversos proveedores de servicios de certificación. 3. Imponer las sanciones establecidas en la presente ley. 4. Crear, actualizar y custodiar la Sección del Registro de los Proveedores de Servicios de Certificación, el cual dependerá del Registro de Electricidad y Telecomunicaciones y deberá estar disponible para consultas del público. 5. Verificar e inspeccionar que los proveedores de servicios de certificación cumplan con los requisitos contenidos en la presente ley, su reglamento y demás normas técnicas aplicables. 6. Supervisar las actividades de los proveedores de servicios de certificación conforme a esta ley. 7. Imponer, recaudar y administrar las tasas	Se elimina la palabra “diversos” del numeral 2 del artículo 28 para que se lea así: 2. Validar los certificados de los proveedores de servicios de certificación. Se agrega la palabra “público” al numeral 4 del artículo 28 para que se lea así: 4. Crear, actualizar y custodiar la Sección del Registro Público de los Proveedores de Servicios de Certificación, el cual dependerá del Registro de Electricidad y Telecomunicaciones y deberá estar disponible para consultas del público”.	**Sugiere la Superintendencia de Valores que se elimine la palabra “diversos” del numeral 2 del artículo 28.** **La misma Superintendencia de Valores sugiere en el Numeral 4 que se indique que el Registro creado es de carácter “público”. Al respecto sugiere incluir en el numeral los principios registrales (principio de prelación, tracto sucesivo, etc.). También sugiere la creación de la figura del “registrador”.**	**La sugerencia se avala, corresponde eliminar la palabra “diversos” que le quita tecnicismo a la regulación y da precisión en cuanto al sentido de lo normado.** **En cuanto al calificativo de “público” del Registro también debe acogerse, tomando en cuenta que se tratará de un registro de acceso público, con atención a todos los principios registrales. En cuanto a la referencia a ello, sin embargo, se considera que no es necesario pues tales principios son connaturales a la materia registral. Además se trata de una dependencia anexa al Registro ya existente en SIGET.**

establecidas en la 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 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 o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones. 13. Seleccionar los expertos técnicos, legales y económicos que considere necesarios para facilitar el ejercicio de sus funciones. 13. Seleccionar los expertos técnicos, legales y económicos que considere necesarios para facilitar el ejercicio de sus funciones. 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. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en esta ley. 16. Las demás que establezca la presente ley y su reglamento.	Cambiar la palabra “seleccionar” en el numeral 13 del artículo 28 para que se lea de la siguiente manera: 13. Contratar los expertos técnicos, legales y económicos que considere necesarios para facilitar el ejercicio de sus funciones.”	**Sugiere la Superintendencia de Valores que en vez del verbo “seleccionar” se hable de “contratar” para darle mayor fuerza al presupuesto asociado a esta Gerencia, dentro de la SIGET.**	**La sugerencia de la Superintendencia de Valores es plenamente viable y se acoge por las razones que ella misma apunta.**
Auditorías e Inspecciones Art. 29.- Para el correcto cumplimiento de las atribuciones concedidas por esta ley, la SIGET realizará, directamente o por contratación, auditorías anuales de los proveedores de servicios de certificación, y podrá ordenar en cualquier momento las	Se cambia la redacción del artículo 29 para que a continuación se lea: “Auditorías e Inspecciones Art. 29.- Para el correcto cumplimiento de las atribuciones concedidas por esta ley, la SIGET realizará, directamente o por	**Sugiere la Superintendencia de Valores una mejora de la redacción del artículo 29.**	**Se acoge la nueva redacción para el artículo 29 sugerida por la Superintendencia de Valores.**

inspecciones que considere necesarias para la verificación del cumplimiento de las obligaciones establecidas de aquéllas. Las auditorías causarán el pago de una tasa señalada en el artículo siguiente y la inspección será a cargo de SIGET y no causará tasa alguna. **Tasa de fiscalización por auditorias** Art. 30.- La tasa de fiscalización por auditorías será cobrada por la SIGET tomando en cuenta el costo de la auditoria más el cien por ciento de su valor Los proveedores de servicios de certificación constituidos por Instituciones del Estado, debidamente acreditados y siempre que sea con la finalidad de otorgar firma electrónica a funcionarios públicos, estarán exentos del pago de las tasas previstas en este artículo. **Medidas para garantizar los servicios de certificación** Art. 31.- La SIGET podrá adoptar las medidas preventivas necesarias para garantizar la confiabilidad de los servicios prestados por los proveedores de servicios de certificación. A tal efecto, podrá dictar las normas técnicas necesarias y entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.	contratación, auditorias anuales a los proveedores de servicios de certificación, y podrá ordenar en cualquier momento las inspecciones que considere necesarias para la verificación del cumplimiento de las obligaciones establecidas a los proveedores de servicios de certificación.		**Sin duda, el requisito de experiencia en la prestación de servicios de certificación debe verificarse, ya que es una garantía adicional para los consumidores de este tipo de servicios.** **Lleva razón por su parte la Superintendencia de Valores en cuanto al tema de que las condiciones de capacidad técnica, de experiencia, capacidad económica y de fianza, deben ser exigidos durante toda la vida útil de la empresa de certificación. A este respecto debería agregarse un aspecto en ese sentido al inicio del artículo ratificando que dichos requisitos deben mantenerse mientras la actividad de la empresa se mantenga. De todos modos el artículo 36 ratifica este hecho, pero conviene subrayar dicha**

Requisitos generales Art. 32.- El servicio de certificación sólo podrá ser prestado por aquella persona o personas, naturales o jurídicas, públicas o privadas, que demuestren cumplir con los siguientes requisitos: a) Tener suficiente capacidad técnica para garantizar la seguridad de las claves pública y privada así como la calidad y 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 en la materia y experiencia en el servicio a prestar comprobable. c) La capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación. En el caso de Instituciones del Estado, éstas deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad. d) Rendir fianza por el monto de doscientos cincuenta mil dólares con el objetivo de indemnizar los daños y perjuicios que pudieren ocasionarse a los usuarios de los servicios de certificación, la cuál será revisada anualmente tomando en cuenta la variación del patrimonio social y el índice de precios al consumidor, e) Presentar un pliego tarifario de los servicios que brindarán a los usuarios. f) Un 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, especialmente lo relacionado a las claves públicas otorgadas así como a los certificados electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos. g) Garantiza, a solicitud del usuario, la suspensión o la cancelación de los	Corregir la redacción del Artículo 32 para que se lea su primer párrafo de la siguiente manera: **Requisitos Generales** Art. 32.- El servicio de certificación sólo podrá ser prestado por aquella persona o personas, naturales o jurídicas, públicas o privadas, que demuestren cumplir con los siguientes requisitos, no sólo a la fecha de su inscripción sino durante toda el periodo en que se presten los servicios de certificación:…" Se sugiere un cambio de redacción a los literales c) y d) y g) del artículo 32, para que a continuación se lean de la siguiente manera: c) La capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación. La mencionada capacidad 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 Gerencia de Servicios de Certificación, mediante las auditorías y estudios que considere convenientes, 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 que se emitirá. 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	**Considera CONAMYPE que hay demasiada discrecionalidad en esta disposición y que, por otra parte, no se puede solicitar experiencia en el servicio a prestar si en el país no existe actualmente este servicio**. **La Superintendencia de Valores considera que los requisitos del artículo 32 deberían de exigirse por todo el periodo de funcionamiento de las empresas de certificación y no únicamente para su inscripción como tales**. **En cuanto a la literal c) sugiere la Superintendencia de Valores que se defina qué se entiende por "contar con capacidad económica y financiera"** **También sugiere la Superintendencia de Valores que se le dé potestad a SIGET para solicitar incrementos al monto definido para la fianza, en función de los riesgos que asuma el proveedor. Es importante asociar la fianza a los riesgos y no a la variación del IPC**.	**circunstancia.** **Las dos sugerencias hechas por la Superintendencia de Valores son de recibo y se ha propuesto una redacción para dichos literales conforme a tales sugerencias. Se ha eliminado el monto de 250000 dólares que se había definido como fianza fija para prestar los servicios que podría ser un elemento que pudiera desestimular a eventuales interesados nacionales o extranjeros en la prestación de servicios de certificación.** **Se ha hecho hincapié en la necesidad de que tanto la fianza como la capacidad económica tenga elementos más detallados para su medición en el Reglamento que se emita al respecto.**

certificados electrónicos que proporcione, de forma rápida y segura; y. h) Satisfacer los demás requisitos previstos en esta ley	certificación. g) Garantizar, a solicitud del usuario, la suspensión o la cancelación de los certificados electrónicos que proporcione, de forma rápida y segura;		
Acreditación de los Proveedores de Servicios de Certificación Art. 33.- La acreditación de los proveedores de servicios de certificación será solicitada por el interesado que se encuentre previamente registrado como operador de redes comerciales, quien además deberá presentar un perfil técnico y económico en el que se refleje el cumplimiento de los requisitos expuestos en el artículo 32, los cuáles serán verificados por la SIGET a través de una auditoría inicial cuyo costo será sufragado previamente por el solicitante. En relación a las exigencias indicadas en los literales a y b del artículo 32, el solicitante acreditara 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 Superintendencia. Si transcurrido el plazo indicado, el solicitante no hubiere cumplido el compromiso indicado, se procederá inmediatamente a dejar sin efecto la acreditación otorgada. El plazo de duración de la acreditación será por tiempo indefinido. La SIGET avalará el pliego tarifario que sea presentado por los proveedores de los	Se corrige la redacción del artículo 33, para que se lea como sigue: **Acreditación de los Proveedores de Servicios de Certificación** Art. 33.- Los Proveedores de Servicios de Certificación presentarán ante la Gerencia de Acreditación de Servicios de Certificación de SIGET, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo 32. El cumplimiento de los requisitos será verificado por la Gerencia de Acreditación a través de una auditoría inicial cuyo costo será sufragado por el solicitante. En relación a las exigencias indicadas en los literales a y b del artículo 32, 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 Superintendencia. Si transcurrido el plazo indicado, el solicitante no hubiere cumplido el compromiso indicado, se procederá inmediatamente a dejar sin efecto la acreditación otorgada. El plazo de duración de la acreditación será	**Pregunta la Superintendencia de Valores de por qué se restringe a los interesados a estar "previamente registrado como operador de redes comerciales".** **CONAMYPE, por otra parte, sugiere que el plazo de autorización no puede ser por tiempo indeterminado que debería pensarse en un plazo entre un año o dos años para la autorización.**	**Esta pregunta no tiene respuesta, desde que este requisito no se explica en un sistema de libre participación y ser parte de redes comerciales sería un compromiso adicional que no agrega nada a la garantía de calidad, certeza y operatividad del proveedor, debe corregirse la redacción en consecuencia.** **En cuanto a la duración de la autorización, personalmente no se aprecian problemas en dejar la autorización por plazo indefinido, sino podría entrarse en la dificultad de obligar a los proveedores a asumir nuevos costos cada vez que procedan a renovar sus vínculos. En todo caso habrá auditorías frecuentes de los servicios que prestan los proveedores, por lo que en cualquier momento que se note que se incumplen los requisitos legales habría consecuencias para ellos, entre ellos la suspensión y la revocación de la autorización.**

servicios de certificación el cual deberá establecerse empleando un modelo basado en costos que sean razonables, no discriminatorios y transparentes.	por tiempo indefinido. La SIGET avalará el pliego tarifario que sea presentado por los proveedores de los servicios de certificación el cual deberá establecerse empleando un modelo basado en costos que sean razonables, no discriminatorios y transparentes".		
Funcionamiento de los Proveedores de Servicios de Certificación extranjeros Art. 34.- Los proveedores de servicios de certificación extranjeros podrán realizar actividades en el país y sus certificados tendrán validez solo sí estuviere avalado mediante un proveedor de servicios de certificación nacional debidamente acreditado.	Se corrige la redacción del artículo 34 para que a continuación se lea como sigue: **Funcionamiento de los Proveedores de Servicios de Certificación extranjeros** Art. 34.- Los proveedores de servicios de certificación extranjeros podrán realizar actividades en el país y sus certificados tendrán la misma validez y eficacia jurídica reconocida por esta ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en esta ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, la seguridad, la validez y la vigencia del certificado. Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en la presente ley, carecerán de los efectos jurídicos que se atribuyen legalmente conforme a esta normativa, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica."	**En relación al artículo 34 señala la Superintendencia de Valores que su redacción debe clarificarse.** **Igualmente se indica que no queda claro que los certificados emitidos por proveedores extranjeros serán simplemente "avalados" por un proveedor nacional, de donde surgen varias dudas: ¿en qué consistirá el aval? ¿Cuál será el mecanismo por medio del cual un proveedor nacional deberá solicitar la acreditación señalada? ¿Cuáles serán las acciones que tomará SIGET para garantizar que el proveedor extranjero cumpla con los requisitos mínimos establecidos por la ley?** **En el mismo sentido van las observaciones de CONAMYPE en cuanto a los proveedores extranjeros.**	**Hemos preferido, siguiendo la recomendación de la Superintendencia de Valores, la redacción de la ley venezolana, en el sentido de que no se da un aval sino que se <u>garantizan</u> conforme a los requerimientos legales los certificados extranjeros mediante la intervención de un Proveedor debidamente autorizado. Si el certificado <u>no ha sido garantizado</u> por la intervención de este Proveedor autorizado, simplemente servirá el mismo como un elemento probatorio valorable conforme a las reglas de la sana crítica, pero sin los efectos jurídicos previstos en esta ley. La pregunta sobre la acción de SIGET se contesta por sí misma, ya que su acción es sobre los proveedores autorizados que dan garantía de los certificados extranjeros. La forma de hacerlo es mediante la figura de la compra de servicios y de la representación.**

Inicio de las actividades del Proveedores de Servicios de Certificación Art. 35.- El proveedor de servicios de certificación acreditado que inicie sus actividades, deberá dar notificación de este hecho a la Gerencia de Acreditación de Servicios de Certificación a más tardar diez días hábiles con antelación al mismo.	Se sugiere la siguiente redacción del artículo 35: **Inicio de las actividades del Proveedor de Servicios de Certificación** Art. 35.- El proveedor de servicios de certificación acreditado que inicie sus actividades, deberá dar notificación de este hecho a la Gerencia de Acreditación de Servicios de Certificación a más tardar diez días hábiles previos a dicho inicio".	**La Superintendencia de Valores sugiere una nueva redacción para el artículo 35.**	**Se sugiere mejorar la redacción del artículo 35 para ratificar que la notificación debe darse diez días hábiles previos al comienzo formal de las actividades de certificación.**
Obligación de Notificación Art. 36.- 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 puede ser mantenida deberá notificarse de inmediato a la Gerencia de Acreditación de Servicios de Certificación.		**La Superintendencia de Valores indica que el inciso segundo del artículo 36 refiere que si "esta garantía de cumplimiento ya no puede ser mantenida"; pero no queda claro a cuál garantía se refiere.**	**Se refiere a la fianza que deberá rendirse, económica, como garantía de daños y perjuicios. Es lógico suponer que si la empresa ya no puede mantener un estándar de calidad conforme a los requerimientos legales salvadoreños y los estándares de calidad internacionales esto deteriora el servicio que se está prestando y podría generar daños y perjuicios para los usuarios de este proveedor, por lo que este, con antelación a causar estos daños debe notificar que tendrá una cesación de sus servicios para proceder a resguardar los intereses ciudadanos y realizar los trámites correspondientes para la cesación de sus servicios resguardando, además, la validez y eficacia de los certificados emitidos al amparo de la ley y en el periodo en que la compañía satisfacía los estándares.**

Suspensión Temporal Voluntaria Art. 37.- El Signatario podrá solicitar la suspensión temporal del servicio de certificación de la firma electrónica, en cuyo caso su proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el signatario, sin que por ello se reste validez a los actos jurídicos firmados con anterioridad a la suspensión.	Se sugiere el siguiente cambio en el art. 37: **Suspensión Temporal Voluntaria** Art. 37.- El Signatario podrá solicitar la suspensión temporal del certificado electrónico, en cuyo caso su Proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el signatario".	**La Superintendencia de Valores cuestiona el eventual uso de este artículo, por lo que sugiere su eliminación del proyecto.**	**Tiene razón la Superintendencia de Valores y el problema proviene de la redacción que alcanzó el proyecto, ya que en la versión original solo se refería a la suspensión temporal del certificado electrónico emitido, solicitud que puede hacer el signatario del certificado y para cumplir fines personales de este, y se sugiere volver a ese sentido original del artículo.**
Obligaciones de los Proveedores Art. 38.- Los proveedores de servicios de certificación tendrán las siguientes obligaciones: a) Inscribir el nombre de dominio en el registro correspondiente bajo el sufijo .sv. b) Adoptar las medidas necesarias para determinar la exactitud de los certificados electrónicos que proporcionen, la identidad y la calidad del signatario. c) Garantizar la validez, vigencia, legalidad y seguridad del certificado electrónico que proporcione. d) Garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas que proporcionen. e) Verificar la información suministrada por el signatario. f) Crear y mantener un archivo de certificados en medios electrónicos para su consulta por un plazo indefinido. g) Sin perjuicio de otras obligaciones establecidas en la Ley de Protección al Consumidor, deberá informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su página web en la Internet y a través de cualquier otra forma de acceso público, los términos precisos y condiciones para el uso	Se sugiere un cambio en la redacción del inciso f) del artículo 38: f) Crear y mantener un archivo de los certificados emitidos en medios electrónicos para su consulta por plazo indefinido". Se sugiere un cambio en la redacción del inciso g) del artículo 38: g) Sin perjuicio de otras obligaciones establecidas en la Ley de Protección del 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".	**La Superintendencia de Valores sugiere cambiar la redacción del inciso c) agregando que se garantizará también la "unicidad" del certificado.** **La Superintendencia de Valores también sugiere cambios en la redacción del inciso f) del artículo 38.** **La Superintendencia de Valores también sugiere cambios en la redacción del inciso g) del artículo 38.**	**En el derecho comparado no se ha incluido la garantía de que el certificado es "único" quizá porque tecnológicamente el signatario otorga el certificado, pero nada impide, que él decida emitir otros más, caso en el cual que quien está afectando la condición propia del certificado no es él sino el signatario mismo, caso en el cual que la garantía podría perder vigencia por el propio dolo del signatario.** **Tecnológicamente hablando se emite un certificado, con un número único y un consecutivo protegido informáticamente, esa es la garantía que se tiene. Si el signatario decide emitir otros nada se lo impide pero si esto causa conflicto sería él quien tiene que responder por la existencia de varios certificados emitidos.** **El cambio se admite. No hay duda que el archivo que se llevará puntualmente es el de los certificados admitidos, y con el cambio sugerido se mejora la redacción del inciso f) del art. 38.** **Los cambios sugeridos mejoran la redacción del inciso g) del artículo 38.**

del certificado electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia. h) 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. i) 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 dichos certificados electrónicos. j) Dar aviso a la Fiscalía General de la República cuando en el desarrollo de sus actividades tenga indicios del cometimiento de un delito. k) 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. l) Renovar anualmente la fianza establecida en el Art. 32 literal d) previo su vencimiento. ll) 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. 39.- 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 concederá el plazo máximo de dos meses para suplir dichas deficiencias. En caso de no suplir dichas deficiencias dos auditorías sucesivas, se aplicarán las sanciones previstas en esta ley.	Se sugiere una mejora en la redacción del párrafo segundo del artículo 39: “En caso de suplir dichas deficiencias en dos auditorías sucesivas, se aplicarán las sanciones previstas en esta ley”.	**La Superintendencia de Valores también sugiere cambios en la redacción del artículo 39, párrafo dos.**	**Los cambios sugeridos mejoran la redacción del párrafo segundo del artículo 39.**
Responsabilidad por daños y perjuicios Art. 40.- Los proveedores de servicios de certificación serán responsables de los daños y perjuicios que ocasionen a los usuarios de sus servicios 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 para el cumplimiento de sus funciones. Para la responsabilidad por daños y perjuicios se observará el derecho común, sin embargo, le corresponderá al proveedor de servicios de certificación probar la debida diligencia. Lo dispuesto en el presente artículo será extensivo al supuesto en que el proveedor local hubiere avalado el servicio del Proveedor de servicios de certificación extranjero, en los términos expuestos en el artículo 34.	Se sugiere un cambio en la redacción del párrafo final del artículo 40: Lo dispuesto en el presente artículo será extensivo al proveedor de servicios de certificación local que hubiere garantizado el certificado emitido por un proveedor extranjero, en los términos expuestos en el artículo 34.	**La Superintendencia de Valores también sugiere cambios en la redacción del último párrafo del artículo 40.**	**Por los cambios hechos en el artículo 34 debe hacerse previsión en el artículo 40, último párrafo, que el proveedor local que garantiza un certificado emitido por un proveedor extranjero asume responsabilidades de conformidad con el artículo 40, lo que aclara la redacción y mejora el sentido jurídico de dicha norma. Los cambios son de recibo, se incluyen.**

Notificación del cese de actividades Art. 41.- Cuando los proveedores de servicios de certificación decidan cesar en sus actividades, lo notificarán a la Gerencia de Acreditación de Servicios de Certificación, al menos con noventa días de anticipación a la fecha de cesación. La Gerencia de Acreditación de Servicios de Certificación después de haber recibido la notificación, emitirá un resolución dentro de las siguientes setenta y dos horas, 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 Gerencia de Acreditación de Servicios de Certificación ordenará al proveedor que realice los trámites necesarios para hacer del conocimiento de los usuarios y del público en general, de 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 traspaso a otro proveedor o bien, deberá notificar a los usuarios, para que tomen conocimiento de la extinción de sus certificados, y a SIGET.	Se sugieren cambios en la redacción del segundo párrafo del artículo 41: La Gerencia de Acreditación de Servicios de Certificación después de haber recibido la notificación, emitirá una resolución dentro de las 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 Gerencia de Acreditación de Servicios de Certificación ordenará al proveedor que realice los trámites necesarios para hacer del conocimiento de los usuarios y del público en general, de la cesación de esas actividades y para garantizar la conservación de la información. Se sugiere cambios en la redacción del párrafo tercero del artículo 41, para que se lea de la siguiente manera: 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 traspaso a otro proveedor, deberá notificar a los usuarios y a la SIGET a través de su Gerencia de Servicios de Certificación, para que realicen las gestiones correspondientes para la extinción de los certificados.	**La Superintendencia de Valores también sugiere ligeros cambios en la redacción del párrafo segundo del artículo 41.** **La Superintendencia de Valores también cambios en la redacción del párrafo tercero del artículo 41.**	**Los cambios son de recibo, se incluyen.**

El proveedor de servicios de certificación deberá trasladar a SIGET el archivo de certificados en medio electrónico a que se refiere la letra f) del Art. 38. En todo caso, el cese de las actividades de un proveedor de servicios de certificación conllevará su cancelación del registro llevado por la Gerencia de Acreditación de Servicios de Certificación así como el pago de las obligaciones económicas pendientes derivadas de sus funciones.			
Garantía de la Autoría de la Firma Electrónica Art. 42.- El certificado electrónico garantiza la autoría de la firma electrónica así como la autenticidad, integridad, confidencialidad y no repudiación del documento electrónico. Si el certificado electrónico no garantiza la autoría y demás características antes dichas, por alteración o cualquier otra razón, el documento electrónico carecerá de validez.	Se sugiere un ligero cambio a la redacción del último párrafo del artículo 42: **Garantía de la Autoría de la Firma Electrónica** Art. 42.- El certificado electrónico garantiza la autoría de la firma electrónica así como la autenticidad, integridad, confidencialidad y no repudiación del documento electrónico. La falta de cualquiera de los requerimientos anteriores invalidará dicho certificado.	**La Superintendencia de Valores también cambios en la redacción del párrafo último del artículo 42.** **CONAMYPE sugiere en relación con este mismo artículo que debería de establecerse la obligación de que si la empresa ha autorizado certificados que no cumplen con los requisitos establecidos por la ley, será cancelada su autorización y se informará a la Fiscalía General de la República para que inicie el proceso penal correspondiente.**	**Los cambios son de recibo, se incluyen. En cuanto a las inquietudes de CONAMYPE debe decirse, en primer lugar, que no habría un delito concreto que abarque dicho comportamiento de un proveedor de servicios de certificación, por lo que la denuncia sería inútil (esto refleja la necesidad de pensar ya la necesidad de un capítulo de delitos informáticos derivados del incumplimiento de requisitos dolosamente), por otra parte, no necesariamente el incumplimiento es doloso también podría ser culposo, por lo que se podrían aplicar las disposiciones administrativas sancionatorias previstas en el proyecto.**
Vigencia del Certificado Electrónico Art. 43.- El proveedor de servicios de certificación y el signatario, de mutuo acuerdo, determinarán la vigencia del certificado electrónico.		**La Superintendencia de Valores sugiere establecer un plazo máximo de vigencia, para que con ello se pueda garantizar la verificación de los datos del titular con una frecuencia mínima.**	**En realidad, el principio de consentimiento y de autonomía de voluntad, que están a la base de una ley de firmas electrónicas, obligan a conservar el principio general de que será el signatario el que, en conjunto con el proveedor de servicios, será el que defina el plazo de vigencia del certificado, lo que va en beneficio de sus intereses.**

Cancelación del Certificado Electrónico Art. 44.- El certificado electrónico de la firma electrónica puede ser cancelado por resolución judicial o del Ministerio Público de conformidad con el ordenamiento legal. Asimismo puede ser cancelado por resolución razonada emitida por la SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación, 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 de aviso al proveedor del hurto, destrucción o extravío del certificado electrónico.	Se sugiere un cambio en la redacción del numeral 3 del artículo 44. 3. Que el signatario dé aviso al proveedor del hurto, destrucción o extravío del certificado electrónico. En tal caso, el proveedor de servicios de certificación procederá inmediatamente a la cancelación del certificado.	**Indica CONAMYPE que lo regulado en este artículo linda con el delito de falsedad material.** **La Superintendencia de Valores sugiere cambios en el artículo 44, numeral 3, en el sentido de que debería de actuarse inmediatamente a cancelar el certificado en tal hipótesis.**	**Es posible, pero en tal caso le correspondería al Ministerio Público y a las autoridades competentes procurar la enervación del proceso penal para la indagación de este delito.** **El comentario de la Superintendencia de Valores es de recibo y merece su inclusión en el proyecto de ley. Ya que si es el propio signatario quien tiene noticia del hurto, destrucción o daño del certificado o su extravío, ante esta noticia debe actuarse inmediatamente para velar por sus derechos e intereses en juego.**
Procedimiento para la cancelación de un certificado electrónico Art. 45.- La SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación, previa denuncia del interesado o de oficio, ordenará audiencia por tres días 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 la 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.		**La CONAMYPE sugiere que en este artículo no se considera a la persona que recibe el certificado.**	**Si se observa el sentido jurídico de la regulación es una especie de ejercicio del derecho del consumidor que es de resorte exclusivo de quien emite el certificado y su signatario. Es decir que lo que se resuelva directamente involucrará a estas partes. La persona que recibió el certificado de buena fe siempre podrá alegar civil y penalmente esta buena fe.**

Contenido de los Certificados Electrónicos Art. 46.- Los certificados electrónicos deberán contener la siguiente información: 1. Identificación del proveedor de servicios de certificación que proporciona el certificado electrónico, indicando su domicilio y dirección electrónica. 2. Fecha de la acreditación y caducidad asignada al proveedor de servicios de certificación por la SIGET por medio de la Gerencia de Acreditación de Servicios de Certificación. 3. Identificación del titular del certificado electrónico, indicando su domicilio y dirección electrónica. 4. La clave pública del titular del certificado. 5. Las fechas de inicio y vencimiento del periodo de vigencia del certificado electrónico." 6. El Algoritmo empleado para la generación de la firma electrónica. 7. Un serial único de identificación del certificado electrónico. 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.	Sugerir un cambio al numeral 7 del art. 46: 7. Un código único de identificación del certificado electrónico. Se sugiere la inclusión de un numeral 10 en el artículo 46, que se leerá de la siguiente manera: “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”. Se sugiere una nueva redacción para el numeral 7 del artículo 48, para que se lea: “7. A que el proveedor no proporcione servicios de calidad inferior ni adicionales a los que haya pactado, y a no recibir publicidad comercial de ningún tipo por medio del proveedor, salvo autorización expresa del usuario en todos los casos señalados;”	**La Superintendencia de Valores sugiere cambios en el numeral 7 del artículo 46, en el sentido de cambiar “serial” por el “código” de identificación.** **La Superintendencia de Valores sugiere incluir un numeral más que se refiera a la relación de presentación, en cuanto la documento legal habilitante del mandato para actuar en representación de alguien o de una persona jurídica.**	**Lo propuesto por la Superintendencia de Valores puede aceptarse. Usualmente este código asignado es serial o consecutivo, pero la palabra código es más entendible.** **La sugerencia es única en su especie en las leyes de firma electrónica que se tuvieron a la vista para la formulación de este Anteproyecto, pero puede ser una buena idea y dota de especial garantía en los casos de mandato o representación. Se acoge la sugerencia.**

Art. 47.- Los certificados electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida, siempre que cumplan con lo requerido en la presente ley y su reglamento Los certificados electrónicos extranjeros, no garantizados por un proveedor de servicios de certificación debidamente acreditado, carecerán de los efectos jurídicos que se atribuyen en la presente ley.			
Derechos de los usuarios Art. 48.- Además de los derechos reconocidos por la Ley de Protección al Consumidor y cualquier otra normativa aplicable, los usuarios o titulares de certificados o firmas electrónicas tendrán los siguientes derechos: 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, así como las reglas sobre prácticas de certificación y los demás que estos se comprometan a seguir en la prestación de los servicios, previamente a que se empiece a efectuar; 2. A la confidencialidad en la información cuando los proveedores de servicios de certificación decidan cesar en sus actividades, 3. A ser informado, 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 del certificado 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 proporcionen la información sobre sus		**La Superintendencia de Valores sugiere mejorar la redacción del numeral 7 del artículo 48, con el objetivo que se clarifique lo allí consignado.** **El BMI sugiere referir al procedimiento sancionatorio administrativo de la Ley de SIGET.**	**La sugerencia es única en su especie en las leyes de firma electrónica que se tuvieron a la vista para la formulación de este Anteproyecto, pero puede ser una buena idea y dota de especial garantía en los casos de mandato o representación.** **Se acoge la sugerencia.** **La sugerencia del BMI es correcta y debe acogerse.**

domicilios en El Salvador; 5. A ser informado, al menos con noventa días de anticipación, por los prestadores de servicios de certificación para los efectos del artículo 41, 6. A traspasar sus datos a otro prestador de servicios de certificación si así lo solicitan, 7. A que el prestador no proporcione más servicios o de calidad inferior de los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario en todos los casos señalados; 8. A que se le respeten los principios y derechos establecidos en el artículo 5 de esta ley. La violación a los derechos previstos en este artículo constituye infracción grave en los términos previstos 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 de acuerdo con el procedimiento previsto en la Ley de Protección al Consumidor en lo que fuere aplicable. **Obligaciones de los usuarios** Art. 49.- Los usuarios o titulares de certificados o firmas electrónicas quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones veraces y completas. Además, estarán obligados a 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.			
Infracciones Art. 50.- Las infracciones a la presente ley se clasifican en graves y menos graves. Son infracciones graves: a) No suplir las deficiencias económicas o técnicas que motivaren las acciones previstas en el Art. 39. b) No renovar las garantías exigidas con el objetivo de garantizar daños y perjuicios que pudieran ocasionarse a los usuarios de servicios de certificación.	Se sugiere cambiar el epígrafe del artículo 50, para que se lea de la siguiente manera: **Infracciones aplicables a los Proveedores de Servicios de Certificación**	**La Superintendencia de Valores sugiere incluir en el epígrafe el detalle que las infracciones que se aplicarán de conformidad con la ley van dirigidas a los proveedores de servicios de certificación.**	**La sugerencia tiene sentido desde que se trata de derecho sancionatorio administrativo y conviene referir claramente que las disposiciones punitivas van dirigidas a los proveedores de servicios de certificación y en el marco de sus actividades.** **El procedimiento sancionatorio administrativo debe estar definido por ley y es correspondiente seguir el señalado en la Ley de SIGET.**
c) Perder la capacidad para suspender, cancelar o revocar los certificados electrónicos que proporcione, según dictamen emitido por la SIGET. d) No entregar la información requerida en el plazo establecido por la SIGET, inclusive en el desarrollo de una inspección o auditoría e) Brindar información falsa cuando sea solicitada por la SIGET f) Negar el acceso a las instalaciones físicas y sistemas de los proveedores de servicios de certificación. g) Violar el secreto de la comunicación amparada con firma electrónica de sus usuarios. h) No cumplir las resoluciones emitidas por la SIGET de acuerdo a los procedimientos establecidos en esta ley y su reglamento.	Se sugiere incluir dos incisos, el i) y el j) en el artículo 50, para que se leerán de la siguiente manera: i) Revelar información personal de sus clientes a terceros, sin el consentimiento expreso de éstos, salvo en los casos en que está obligado por ley. j) El quebrantamiento de lo dispuesto en el artículo 5 sobre el tratamiento de datos personales.	**Sugiere la Superintendencia de Valores incluir un inciso i) donde se considere infracción grave el revelar información personal de los clientes. También se sugiere considerar infracción grave incumplir lo dispuesto por el artículo 5 del Anteproyecto sobre el Tratamiento de Datos Personales.**	**La propuesta es plenamente viable ya que, en efecto, una de las infracciones más graves es precisamente la revelación sin consentimiento de la información personal de los usuarios de los servicios de certificación. Lo mismo debe decirse de la recomendación en cuanto a considerar infracción grave afrentar las disposiciones que sobre tratamiento de datos personales se consigna en el artículo 5. Afectar las expectativas jurídicas de los ciudadanos a este respecto constituye una afrenta grave y antijurídica que debe ser sancionada gravemente. En el caso de afectaciones dolosas debería de consignarse igualmente un delito informático en el marco del Código Penal Salvadoreño. La sugerencia de la Superintendencia de Valores es plenamente compatible con el sentido de la norma y por ello se acoge para darle mayor claridad a lo allí normado.**
Son infracciones menos graves: a) No informar al usuario las características técnicas del certificado adquirido. b) No cancelar las obligaciones económicas derivadas de la presente ley. c) La violación culposa del secreto de la comunicación amparada con firma electrónica de sus usuarios.	Se sugiere incluir un último párrafo en el artículo 50: Las infracciones descritas en este artículo y en el artículo siguiente se tramitarán conforme al procedimiento Administrativo sancionatorio establecido en la Ley Orgánica de SIGET.		

Sanciones Art. 51.- Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones: a) Por la comisión de infracciones graves, se impondrá al infractor una multa de entre dieciséis mil trescientos cincuenta dólares hasta ochenta y un mil seiscientos treinta y siete dólares con cincuenta y siete centavos de dólar. En el caso de las infracciones graves de las letras a), b), c) y h) del artículo anterior, se concederá el plazo de hasta dos meses para superar la deficiencia; si vencido dicho plazo, no se superaren las mismas, se dejara sin efecto la acreditación para operar y se aplicarán las reglas previstas para el cese de actividades contenida en el Art. 41. b) Por la comisión de infracciones menos graves, se impondrá al infractor una multa de hasta dieciséis mil trescientos veintisiete dólares con cincuenta y un centavos de dólar. Las infracciones graves llevarán aparejada, a costa del sancionado, la publicación de la resolución sancionadora en un periódico de circulación nacional y en el Diario Oficial, en la página de inicio del sitio web del Prestador de Servicios de Certificación y en el sitio de Internet de la SIGET, una vez que aquélla tenga carácter de firme. El valor de las multas será ajustado con base al índice de precios al consumidor publicado por el Ministerio de Economía, el ajuste se realizará anualmente a partir del primer día hábil del mes de enero.			

Reglamento Art. 52.- El Presidente de la República deberá emitir el reglamento de esta ley, en un plazo no mayor a seis meses contados a partir de su publicación. **Disposición transitoria** Art. 53.- Cualquier persona natural o jurídica que al momento de entrar en vigencia la presente ley se encuentre brindando servicios de certificación, contará con un plazo no mayor de seis meses para adecuarse al cumplimiento de los requerimientos establecidos por la misma a fin de continuar brindando dicho servicio. **Disposiciones Supletorias** Art. 54.- Las disposiciones y procedimientos contenidos en la Ley de Telecomunicaciones podrán aplicarse en lo que fuere pertinente. **Derogatorias** Art. 55.- Derogase los artículos 6 Inc. 3º y 4º, 7 Inc. 2º, 8, 8-A, 8-B, 8-C, 8-D, 8-E, 9 Inc. 1º, 2º y 3º de la Ley de Simplificación Aduanera contenida en el Decreto Legislativo No. 529, de fecha 13 de enero de 1999, publicada en el Diario Oficial No. 23, Tomo 342 de fecha 3 de febrero de 1999. **Vigencia** Art. 56.- La presente ley entrará en vigencia ocho días después de su publicación.			

Para la elaboración de este listado de sugerencias se han tomado en cuenta las observaciones del BMI, del Ministerio de Hacienda, de la Superintendencia de Valores, del Banco Central de Reserva y de CONAMYPE, quienes hicieron un excelente trabajo de análisis y enviaron material de gran calidad para estudiar cambios en la redacción del articulado. Fue gracias a estas sugerencias que se plantean en estas notas, la necesidad del cambio del nombre de la ley, así como la reorientación del objeto de la ley para aclarar los alcances jurídicos del articulado, entre otros aspectos de importancia.

Se nota una preocupación por permitir a los funcionarios del Estado la posibilidad de emitir certificados y firmas electrónicas; un temor, desde nuestro punto de vista, más bien infundado, y que podría malograr los usos más importantes de la firma electrónica, los cuales sin duda impactarán positivamente en las gestiones gubernamentales en todos sus aspectos, especialmente en materia tributaria, bancaria y financiera, de gobierno electrónico, de compras públicas, etc.

Las instituciones que contribuyeron con sus observaciones no omitieron indicar que es indispensable analizar las reformas a otras leyes (entre ellas las de la SIGET) para mejorar la compatibilidad de la ley y las competencias que aquí se están definiendo. Un tema abierto aun a la discusión es el de la creación de la Gerencia de Acreditación y su papel dentro de la SIGET en las competencias que este anteproyecto estaría creando.

Se indicó, y es un tema no resuelto, el de los montos de las sanciones y los criterios que se tomaron en cuenta para la definición de dichos montos. También la fianza que el anteproyecto establece para poder acreditarse como Proveedor de Servicios es muy alta (de 250,000 dólares), lo que podría provocar que muchas empresas con interés en incidir en la materia prefieran no dedicarse a esta actividad, o bien, excluir a potenciales empresas nacionales que disuadidas por esa onerosa inversión eviten incidir en este mercado.

El tema notarial, que ha sido una preocupación siempre presente, parece haberse resuelto en su gran mayoría. Sin embargo, conviene hacer alguna ronda de análisis y discusión con notarios de experiencia para conocer sus opiniones sobre el texto y si alguno de los artículos pudiera provocar alguna distorsión a su trabajo cotidiano. En esencia, nada impide que haya cibernotarios en El Salvador, como tampoco nada impide que un notario sea certificador de firmas electrónicas. Todo depende de la receptividad del mercado notarial a la prestación de estos servicios y a asumir los costos de la infraestructura tecnológica necesaria.

El papel del Poder Judicial y de los jueces fue analizado también, y hay preocupación por las eventuales observaciones e interpretaciones de los juzgadores que afecten la correcta inteligencia de la ley. A este respecto debe decirse que no será la ley la que resuelva los imponderables de la interpretación judicial, sino que habría que trabajar de cerca con el órgano judicial para apoyar la capacitación de los operadores y, de allí, desarrollar materiales educativos e informativos que coadyuven a una buena administración de la justicia en el ámbito del comercio electrónico y del uso de la firma para diversos actos públicos y privados.

Desde la perspectiva del Programa Regional CAFT-DR, cuyo objetivo es la facilitación del comercio y cumplir con los requerimientos del acuerdo regional suscrito por los países que forman parte de él, se cumple con esta meta y el anteproyecto promueve dicha facilitación. Claro está, aún hace falta legislación en comercio electrónico que, junto con la Ley de Firma Electrónica, promocione esta actividad y otras materias que son anexas a ésta.

Sin duda, la ley provocará cambios importantes en la interacción entre el Estado y los particulares; creará nuevas formas de comercio y de interrelación entre los ciudadanos; mejorará el sistema de compras del Estado; le dará el marco legal a las iniciativas de gobierno electrónico que se impulsen y, por supuesto, hará

posible que se creen nuevos nichos de mercado en el campo tecnológico. El despertar de estos nichos de mercado depende de la creación de confianza y de un adecuado marco legal, que ahora se está preparando.

Es posible recabar más opiniones sobre el proyecto, pero sin duda se ha alcanzado un consenso importante de apoyo a esta iniciativa y el articulado ha recibido un remozamiento y perfeccionamiento notable. Hará falta, sin embargo, un estudio detallado de las derogatorias y de la incidencia potencial del proyecto en el orden jurídico salvadoreño para salvar en lo posible las eventuales contradicciones que pudieran generarse.

---

[1] Se sugiere volver al nombre de la ley **LEY DE FIRMAS Y COMUNICACIONES ELECTRÓNICAS**, lo cual es una sugerencia avalada no sólo por la consultoría sino también por las recomendaciones del Ministerio de Hacienda. Debe tomarse en cuenta que el nombre del anteproyecto actual le hace perder mucho de su sentido normativo y no pone especial énfasis en el tema de firma electrónica. Agregar, además, que se refiere a comunicaciones electrónicas, añade muchos aspectos trascendentes que adelantan el interés del legislador en materia de comercio electrónico. El nombre sugerido es, por otro lado, mucho más técnico, aun cuando sería aconsejable incluir en el título la referencia a los mensajes electrónicos, como tales.

[2] El Banco Central de Reserva hace una propuesta de redacción para el principio de Autenticidad, con el fin de garantizar al receptor que el mensaje efectivamente proviene del iniciador o emisor y no de otra entidad. Esta sugerencia, aun cuando es razonable, le da un sentido jurídico diferente al principio de autenticidad desde la perspectiva de la firma electrónica.

[3] El Banco Central de Reserva indica que este Capítulo II, intitulado “Documentos en Soporte Electrónico”, cambia algunas reglas de documentos, por lo que convendría aclarar si lo que se pretende es hacer una división de los documentos electrónicos o si se hace referencia a los ya definidos por el Código Procesal Civil. La verdad es que el anteproyecto, por vía del principio de equivalencia, lo que pretende es hacer una referencia a los documentos ya previstos en la legislación y simplemente extiende la circunstancia de que éstos también podrán consignarse en formato electrónico. Habrá documentos que por sus características requerirán solemnidades y formalidades que sólo podrán satisfacerse mediante documentos escrito; sin embargo, ya eso está señalado en las leyes correspondientes, como en la Ley Familiar en materia de matrimonios, etc. En todo caso, las leyes de firma electrónica de diversos países, como la venezolana, por ejemplo, considera que, en la medida que tales solemnidades y formalidades puedan ser satisfechas, podrían darse mediante los mecanismos planteados por la ley de firmas (cfr. Artículo 6 de la Ley Venezolana del Decreto con fuerza de ley de Mensaje de Datos y Firmas Electrónicas de 2001).

[4] El Banco Central de Reserva indica que nada se ha dicho sobre el tema del uso de estos documentos en sede judicial; sin embargo, ese es un tema que no puede resolverse en esta ley. Será la jurisprudencia y el criterio de los tribunales los que decidirán la forma en que estos documentos serán tratados jurisdiccionalmente, así como la forma en que se entenderá que generarán efectos jurídicos.