UNION INTERNACIONAL
DE
TELECOMUNICACIONES

ASOCIACION DE EMPRESAS
DE TELECOMUNICACIONES
DE LA COMUNIDAD ANDINA

Legislación sobre Comercio Electrónico en los Países Miembros de la Comunidad Andina

Análisis comparativo

Recomendaciones para su armonización

Junio de 2002

Estudio realizado con el apoyo de la Unión Internacional de Telecomunicaciones -UIT-,
Oficina de Desarrollo de las Telecomunicaciones Unidad e-Strategy.

Especialista de la UIT
María Gabriela Sarmiento
Abogado
Administrador de proyectos
Unidad e-Strategy
Telf. +41 22 730 58 95
Fax +41 22 730 54 84
maria-gabriela.sarmiento@itu.int

« …Il faut que les États, à travers une volonté politique commune opèrent un rapprochement de leurs systèmes juridiques sur les questions relatives aux réseaux. Il faut qu'ils accordent sur un socle minimal de valeurs universelles dont il se chargent d'assurer l'application effective. »

« …La nécessité d'une harmonisation repose sur un constat d'inefficacité de carence ou de contradiction des règles existantes. »

« …Deux tentations extrêmes
menacent la qualité de l'harmonisation: celle de la réponse normative en temps réel au défi technologique et celle de l'abandon du droit à la technique. »

« …la régulation du commerce électronique, la mise en place des nouveaux modes d'adressage électronique ne nécessitent pas automatiquement une harmonisation « autoritaire » et « maximale » »

« …l'échelle d'intervention et la nécessaire prudence vis-à-vis des évolutions techniques conduisent naturellement à privilégier l'élaboration d'une norme générale, fixant davantage des standards que des règles précises. »

« …La complétude de l'harmonisation ne sera pas nécessairement recherchée au sein d'un texte unique mais dans l'application simultanée de plusieurs corps de règles d'importances et de sources différentes. »

Extractos del artículo: « *Faut-il une harmonisation minimale du droit ?*[1] » de Valérie Laure Benabou, Profesora de la Universidad de Lyon 2, Francia.

[1] Traducción no fidedigna del artículo: ¿Hace falta una armonización mínima del derecho?.
« … Por medio de una voluntad política común, los Estados deben realizar un acercamiento de sus sistemas jurídicos sobre las cuestiones relacionadas con las redes. Ello debe hacerse con fundamento en valores universales básicos. »
« …La necesidad de una armonización reposa en la constatación de ineficacia y carencia de normas existentes o de una contradicción entre las mismas. »
« …La calidad de la armonización de normas es amenazada por dos tentaciones extremas: la respuesta normativa en tiempo real en desafío a la tecnología y el abandono del derecho a la tecnología. »
« …la regulación del comercio electrónico y la puesta en práctica de nuevos usos electrónicos no necesitan de una armonización automática 'autoritaria' y 'extrema' »
« …la escala de intervención y la prudencia necesaria *vis à vis* de las evoluciones técnicas conducen, naturalmente, a privilegiar la elaboración de una norma general que establece estándares en lugar de crear reglas precisas. »
« …la armonización no será fruto de un texto único, sino de la aplicación simultánea de varios cuerpos legales de importancia y de diversas fuentes. » Traducción nuestra.

Indice

Anexos

Anexo A:

Cuadro comparativo de los textos legales sobre comercio electrónico en los países de la Comunidad Andina

Anexo B:

Legislación vigente sobre comercio electrónico en los Países Miembros de la Comunidad Andina y anteproyectos Bolivianos

Anexo C:

Lista, no exhaustiva, de Entidades / Autoridades de Certificación

Introducción

El objetivo de este trabajo es realizar un estudio de derecho comparado de la legislación vigente y proyectos de ley sobre comercio electrónico en los países de la Comunidad Andina y presentar un conjunto de recomendaciones con el propósito de contribuir a la armonización de disposiciones legales en esta materia. Actualmente, los Países Miembros de la Comunidad son: Bolivia, Colombia, Ecuador, Perú y Venezuela.

Las áreas cubiertas por este trabajo son las siguientes: los principios generales acogidos por las legislaciones de comercio electrónico, los mensajes de datos, las firmas electrónicas (incluyendo firmas digitales), los certificados digitales y las Entidades / autoridades de Certificación y Registro.

Este trabajo se llevó a cabo en la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la Unión Internacional de Telecomunicaciones (UIT), a solicitud de la Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (ASETA), en consonancia con una de las prioridades de la BDT / UIT, cuya intención es "Promover un entorno jurídico favorable para los ciber-servicios / aplicaciones: Los ciber-servicios / aplicaciones requieren un marco jurídico y de política adecuado para contemplar aspectos tales como la privacidad de los datos, la prevención de los ciber-crímenes, la seguridad, las cuestiones de orden ético, las firmas electrónicas, las facultades de certificación y los contratos electrónicos, a efectos de crear un clima de confianza, proteger los derechos de las partes y fomentar su utilización. Es preciso realizar actividades para ayudar a los países en desarrollo en ámbitos concretos relacionados con el marco jurídico de los ciber-servicios / aplicaciones electrónicos, teniendo en cuenta las actividades del Programa de Reforma Reglamentaria y estableciendo una estrecha colaboración en las esferas correspondientes para evitar superposiciones y garantizar una utilización eficaz de los recursos".

"ASETA es una asociación de empresas operadoras de servicios de telecomunicaciones que en el marco de la Comunidad Andina coadyuva al desarrollo armónico de las telecomunicaciones, contribuyendo así con el proceso de integración.

Es un organismo internacional, sin fines de lucro, creado por recomendación de la Primera Reunión de Ministros de Comunicaciones del Acuerdo Subregional Andino y designado por el Comité Andino de Autoridades de Telecomunicaciones (CAATEL)[2] como Organismo Consultivo Permanente." La sede de la Secretaría General de ASETA se encuentra en Quito – Ecuador.

Algunos de los objetivos de ASETA en relación con la Comunidad Andina de Naciones son los siguientes:

a. apoyar y orientar a la Secretaría General de la Comunidad Andina (CAN) en el área de las telecomunicaciones para contribuir con el proceso de integración,
b. propiciar la armonización de normas de telecomunicaciones de los Países Miembros, así como el establecimiento de la norma andina,
c. propiciar y contribuir a la cooperación técnica, al intercambio y divulgación de la información científica, legal y contractual, y al desarrollo y difusión de tecnologías en las actividades relacionadas con las telecomunicaciones en la Comunidad Andina, y
d. apoyar la gestión ante Organismos y Agencias Internacionales de cooperación[3], asistencia técnica y financiera para el desarrollo del sector de telecomunicaciones de la Comunidad Andina.

"En ejecución de estos objetivos, ASETA suscribió un Convenio con la Secretaría General de la Comunidad Andina de Naciones, mediante el cual se establecen mecanismos para apoyar el desarrollo de los servicios y de la infraestructura de telecomunicaciones de la Subregión Andina."

---

[2] "El CAATEL, creado por la VI Reunión de Ministros de Transportes, Comunicaciones y Obras Públicas de los Países Miembros del Acuerdo de Cartagena, se encarga de estudiar y proponer políticas andinas de telecomunicaciones, a fin de facilitar la Interconectvidad de los servicios de telecomunicaciones. Este Comité Andino actúa de manera coordinada con ASETA, para hacer compatible y complementarios los lineamientos de las Políticas Sub-regionales de Telecomunicaciones con las expectativas y necesidades de las Empresas Andinas encargadas de las operaciones del sector." A su vez, el CAATEL "asesora a los órganos del Acuerdo de Cartagena en materia de telecomunicaciones, proponiendo a la Comisión, y a la Junta, los proyectos de Decisiones y normas de su competencia, tomando en cuenta las legislaciones nacionales y las normas y recomendaciones aplicables de la Unión Internacional de Telecomunicaciones (UIT)"

[3] "ASETA, como organismo regional de telecomunicaciones, tiene participación en los trabajos de la Unión Internacional de Telecomunicaciones (UIT), con quien suscribió un Convenio de Cooperación."

Retomando el tema objeto de este trabajo, cabe mencionar que el mismo aborda solo una parte de las áreas en estudio, ya que por razones de tiempo, nos hemos visto constreñidos a presentar este primer reporte antes de finalizar el primer semestre de 2002.

El motivo se debe a que la Secretaría General de la Comunidad Andina (CAN) adelanta la preparación de un proyecto de Decisión sobre armonización de las legislaciones de comercio electrónico de sus Países Miembros. Esperamos que dicha Secretaría tome en consideración las recomendaciones presentadas a continuación como parte del vasto material de apoyo que se ha recabado para llevar a cabo tan importante tarea.

Como parte integrante de este trabajo se desarrollan capítulos sobre la importancia y evolución del comercio electrónico en Latino América y el mundo y el proyecto de la UIT con la empresa privada sobre despliegue de Entidades / Autoridades de Registro en países en desarrollo y menos adelantados. Asimismo, encontrarán una lista, no exhaustiva, de las entidades / Autoridades de Certificación existentes en diferentes países.

Recomendaciones para armonizar la legislación vigente de los Países Miembros de la Comunidad en las siguientes áreas: delitos informáticos, protección de datos (*Habeas Data*), defensa al consumidor, derechos de autor, derecho aplicable a transacciones electrónicas, jurisdicción, arbitraje e impuestos a las transacciones electrónicas, serán tratadas en un segundo reporte a ser presentado en el segundo semestre de 2002.

Para concluir esta parte introductoria, nos gustaría traducir al español y reproducir las palabras de Valérie Laure Benabou, profesora de la Universidad de Lión quien considera que si hay una respuesta normativa al reto tecnológico en tiempo real obtendremos legislaciones hechas a la carrera, redactadas precipitadamente y sin concentración. En consecuencia, estas legislaciones serán inexactas pues estarán empapadas de un discurso técnico oscuro y producirán soluciones inadaptadas que han sido redactadas dentro del marco de un estado técnico específico, en el tiempo y en el espacio, considerado anacrónico para el momento en que la nueva legislación es adoptada.

La Profesora Benabou piensa, igualmente, que el abandono del derecho a la tecnología conduce a una transferencia efectiva del poder del Legislador hacia el experto, quien no tiene la misma legitimidad para legislar... "*LA TECNOLOGÍA ES NEUTRA Y 'EL DERECHO' ES QUIEN DEBE ORIENTARLA"*.

Metodología

La primera actividad que emprendimos para realizar el estudio de derecho comparado y elaborar recomendaciones para la armonización de los textos legales vigentes sobre comercio electrónico de la Comunidad Andina, fue identificar cuáles son las diferentes áreas objeto de estudio. La investigación arrojó como resultado las siguientes áreas: servicios de certificación, certificados digitales, Entidades / Autoridades de Certificación, firmas electrónicas (incluyendo firmas digitales), contratos electrónicos y mensajes de datos.

Asimismo, observamos que debíamos abordar áreas directamente relacionadas con el comercio electrónico tales como el derecho aplicable a las transacciones electrónicas, la jurisdicción y el arbitraje, la responsabilidad de los proveedores de servicios de Internet, los delitos informáticos, los impuestos a las transacciones electrónicas, el derecho de autor, la protección de datos (*Habeas Data*) y la defensa al consumidor, entre otros. Tal y como hemos explicado anteriormente, estas últimas no serán objeto del primer reporte de este trabajo.

Seguidamente, realizamos una investigación para determinar cuál era la legislación vigente en los Países Miembros de la Comunidad Andina sobre esta materia. La investigación arrojó los siguientes resultados:

- Bolivia había emprendido una reestructuración de todo su ordenamiento jurídico a fin de adaptar sus disposiciones legales a las necesidades de las nuevas tecnologías de la Información y Comunicación;
- Colombia, Perú y Venezuela adoptaron nuevas legislaciones sobre comercio electrónico, sobre firmas y certificados digitales y sobre mensajes de datos y firmas digitales, respectivamente;
- Ecuador estaba en proceso de aprobar un proyecto de Ley de comercio electrónico que fue aprobado por el Congreso de ese país en febrero de 2002, vetado por el Presidente de la República en marzo y finalmente acogido y publicado como Ley de Comercio Electrónico en Abril.

A pesar de que Colombia tomó como base los lineamientos de la Ley Modelo sobre Comercio Electrónico de la UNCITRAL[4] para adoptar sus propios textos legales, y de que Ecuador y Venezuela siguieron los mismos de cerca, deben realizarse esfuerzos para evitar cualquier contradicción entre la legislación nacional de los referidos Países Miembros de la Comunidad Andina. Y en particular, porque Perú y Bolivia no se basaron en absoluto en el contenido de la Ley Modelo.

La UIT realizó un detallado análisis legal y técnico de la legislación vigente sobre comercio electrónico en estos países. El contenido de la misma fue comparado y las semejanzas y diferencias entre las mismas fueron identificadas. Igualmente, aquellas áreas no incluidas en las legislaciones nacionales han sido tomadas en cuenta para recomendar su incorporación en un eventual texto armonizado.

Aunado a este estudio, tuvimos la oportunidad de visitar cuatro de los cinco Países Miembros de la Comunidad Andina, en donde intercambiamos puntos de vista, críticas y demás comentarios en relación con comercio electrónico y a su regulación con entidades públicas y privadas directa e indirectamente influenciadas por dicha regulación. Gracias al aporte de todas las personas que tuvimos ocasión de visitar, pudimos identificar los temas más controvertidos del ámbito legal del comercio electrónico, como mencionamos al inicio de este trabajo.

Luego de haber asimilado tanto la legislación como la experiencia práctica del contenido de aquélla, hemos pasado a la redacción de recomendaciones inspiradas en un espíritu de armonización. Creemos que las recomendaciones responden a las necesidades de los cinco países. Esta armonización, facilitará las relaciones comerciales realizadas vía medios electrónicos.

Cabe mencionar, que las recomendaciones han sido elaboradas de conformidad con los principios generales de comercio electrónico reconocidos internacionalmente.

Estas recomendaciones no deben ser consideradas, en ningún caso, como una política de la UIT en comercio electrónico.

---

[4] *United Nations Commission for International Trade Law (UNCITRAL)* o Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)

Agradecimiento

La Unión Internacional de Telecomunicaciones y ASETA desean dejar plasmada en este trabajo su profunda gratitud hacia todas aquellas entidades públicas, semi-públicas y privadas e individuos que nos recibieron en Colombia, Ecuador y Perú[5].

Gracias a su invalorable colaboración y preciado aporte, hemos logrado identificar de manera directa los temas más controvertidos en la legislación sobre comercio electrónico de estos tres países.

El intercambio de ideas sostenido durante las múltiples visitas llevadas a cabo durante el mes de marzo de 2002, nos permitió realizar una interpretación más adecuada y pertinente del contenido y espíritu de la legislación objeto de nuestro estudio; y de esta manera, reflejar y unanimizar las opiniones recogidas durante nuestras tres semanas de misión.

Queremos agradecer, especialmente, la colaboración de las siguientes personas en Colombia, Ecuador y Perú, quienes apoyaron a la UIT y a ASETA en la coordinación de las reuniones y entrevistas efectuadas:

Dr. Marco Pérez, Gerente, *Property rights* Consultores Legales. Bogotá – Colombia.
Dr. José Luis Barzallo, Barzallo & Barzallo Abogados. Quito – Ecuador.
Ing. Carlos Vera Quintana, Presidente, CORPECE. Quito – Ecuador.
Ing. Víctor J. Pereyra, Servicios de Comercio Electrónico, LIMATEL. Lima – Perú.

La coordinación general de las actividades realizadas en los países de la subregión andina estuvo a cargo del Ing. Jairo Gómez Malaver, Director de Estudios y Proyectos de ASETA.

A pesar de que el tiempo disponible para la misión en los países andinos, no permitió visitar Bolivia y Venezuela, los ingenieros Marcelo López Arjona, Secretario General y Eduardo Pichilingue Prieto, Director de Relaciones Internacionales, ambos representantes de ASETA, tuvieron la oportunidad de reunirse con el Superintendente de Servicios de Certificación Electrónica de Venezuela y el Presidente de la Cámara Venezolana de Comercio Electrónico (CAVECOM-E). Asimismo, la abogado María Gabriela Sarmiento, Gerente de proyectos de la Unidad e-Strategy del BDT/UIT mantuvo una conversación telefónica con la Dra. Dra. Rosa Laguna Quiroz del Ministerio de Justicia y Derechos Humanos de la República de Bolivia. Agradecemos su amable colaboración y en especial su aporte en este trabajo, ya que su presentación sobre el Marco Regulatorio del Comercio Electrónico en Bolivia es la única fuente que obtuvimos con todos los anteproyectos de Ley previstos para adaptar las normas legales de ese país a las necesidades de las nuevas tecnologías.

ASETA desea resaltar igualmente la colaboración prestada por el Ing. Gabriel Bernal, Administrador de Area de la UIT, para la concreción de este trabajo y la dedicación de la abogado María Gabriela Sarmiento, Gerente de proyectos de la Unidad e-Strategy del BDT/UIT, autora del estudio.

[5] Una lista completa de los organismos visitados se encuentra anexa al presente documento.

Límites de responsabilidad

La UIT pone a disposición del lector este documento bajo los siguientes términos y condiciones de uso. Toda utilización del documento implica aceptación de la siguiente descarga de responsabilidad:

1. Las direcciones de la World Wide Web a las que remite este documento no están bajo el control de **la UIT** y su contenido es responsabilidad de sus respectivos autores o representantes. Al hacer un enlace a un sitio Web, **la UIT** pretende facilitar el acceso a información que podría ser de utilidad para el usuario, pero no se responsabiliza, en ningún caso, de los contenidos ni de ningún resultado derivado de su visita.

2. La remisión o cita de un sitio Web no implica la aprobación por parte de la UIT de los contenidos de dicho sitio, ni tampoco algún tipo de asociación de la UIT con los responsables del mismo.

3. El conocimiento y seguimiento de las condiciones de uso de los sitios Web a los que remite este sitio son responsabilidad de los usuarios.

4. Si alguna organización o entidad no desea que su dirección URL aparezca citada en este documento, solicitamos comunicarlo por escrito para que la misma sea suprimida.

5. El servicio, los datos y la información de este trabajo se entregan al lector sin ningún tipo de garantías, explícitas o implícitas. **La UIT** no garantiza la exactitud, pertinencia, disponibilidad o fiabilidad de la información proveniente de otras fuentes identificadas en este documento.

6. **La UIT** no se responsabiliza por las decisiones o acciones que se tomen a partir de la información propia o de terceros contenidas en este documento, así como tampoco por cualquier consecuencia que se derive del uso de estos datos.

7. Los puntos de vista expresados en el presente trabajo son propios del autor y no reflejan, necesariamente, las opiniones de **la UIT**, de sus Países Miembros, de sus miembros empresariales y estatales ni la de sus empleados.

Parte I: Información General sobre Comercio Electrónico

A. Importancia y evolución del comercio electrónico

Palabras pronunciadas por el Sr. Yoshio UTSUMI, Secretario General de la Unión Internacional de Telecomunicaciones en su exposición titulada "El desarrollo tecnológico no basta" presentada durante el Día Mundial de las Telecomunicaciones del 17 de mayo de 1999:

"De todas las nuevas aplicaciones surgidas desde la incipiente era de la información, el comercio electrónico es quizás la que más potencial tiene de transformar radicalmente las relaciones económicas que definirán nuestra forma de vida en el siglo XXI." "...si queremos que se materialice todo el potencial del comercio electrónico debemos actuar ahora para desarrollar una auténtica infraestructura mundial de la información que permita no sólo cursar nuestras transacciones de forma segura y fiable, sino también rentable.

En la actualidad, la expansión generalizada del comercio en línea sigue estando limitada por barreras asociadas a los costes -por ejemplo el precio de las líneas arrendadas de gran velocidad o las estructuras tarifarias desfasadas que reflejan los antiguos esquemas de llamadas telefónicas. Si los operadores de todo el mundo desean seriamente fomentar el crecimiento del comercio electrónico tendrán que reestructurar las tarifas para que éstas sean reflejo de los nuevos esquemas de utilización sobre la base de los datos, al tiempo que aseguran que el precio del acceso a la infraestructura adecuada de telecomunicaciones es asequible para los usuarios empresariales ordinarios.

El desarrollo de una infraestructura mundial de la información que esté al servicio de las necesidades de toda la población del mundo y no sólo de las naciones de economía más saneada, es uno de los objetivos estratégicos de la Unión Internacional de las Telecomunicaciones. Teniendo esto presente, la UIT intenta desarrollar normas mundiales que abarquen todas las materias, desde las arquitecturas de red avanzada hasta los sistemas de seguridad y los de autorización digital."

"Además, la política y la reglamentación desempeñarán un papel vital desenredando la maraña de aspectos no resueltos que conlleva la implementación del comercio electrónico -aspectos de comercio trans-fronterizo sin restricciones, de arbitraje y resolución de conflictos, de soberanía nacional y de protección del consumidor- o dicho de otra manera, en la creación del tipo de confianza que se necesita para asegurar al mercado de consumo la comodidad de la realización de negocios en línea."

"El comercio electrónico puede representar la mejor oportunidad que le queda al mundo en desarrollo para transformar los modelos económicos desfavorecidos del siglo XX en un marco de comercio mundial en el que puedan participar por igual todos los países."

Extracto del mensaje presentado por el Sr. Yoshio UTSUMI, Secretario General de la Unión Internacional de Telecomunicaciones, durante el Día Mundial de las Telecomunicaciones del 17 de mayo de 1999:

"Para aprovechar plenamente las oportunidades que ofrece el comercio electrónico, los Países Miembros de la UIT deben estar dispuestos a tomar diferentes medidas.

- En primer lugar, deben estar dispuestos a proporcionar un acceso general a las redes y servicios de información, porque éstas son la infraestructura básica de la economía digital.
- En segundo lugar, deben estar dispuestos a abrir sus economías a los inversionistas y abastecedores extranjeros. Éste es un medio indispensable para la participación en el mercado mundial.

- En tercer lugar, y ello es lo más importante, han de estar dispuestos a ofrecer a su población los conocimientos necesarios para la economía de la información, porque sin educación no puede haber innovación y tampoco crecimiento."

Extractos del documento de discusión titulado "Consideraciones de política en relación con el comercio electrónico" presentado durante el Día Mundial de las Telecomunicaciones del 17 de mayo de 1999:

"Lo que ha provocado la reciente concentración del interés internacional en el nuevo mundo del comercio electrónico es la rápida integración de Internet y de otras funciones basadas en la telecomunicación en casi todas las esferas de la vida comercial.

Entre los medios principales que cabe calificar de coadyuvantes al comercio electrónico mundial figuran los siguientes:

- Servicios tradicionales de telecomunicaciones basados en la transmisión de textos, voz y datos, en particular el télex, el facsímil y la llamada telefónica gratuita.
- Servicios en línea más nuevos, basados principalmente en Internet pero que utilizan también otros servicios en línea, como el videotexto.
- La venta de soporte lógico y los servicios de información por transacción o suscripción.

La actividad del comercio electrónico se puede clasificar en cinco grandes grupos:

- De empresa a empresa o *business to business (B2B)* (al por mayor y al por menor).
- De la empresa al consumidor o *business to consumer (B2C)* (venta al por menor al consumidor).
- De las empresas al gobierno *o business to government (B2G)*.
- Del gobierno al consumidor o *government to consumer (G2C)*.
- Del consumidor al consumidor o *consumer to consumer (C2C)*.

Entre los servicios que aprovecharán probablemente la aplicación de las técnicas de comercio electrónico cabe citar: los servicios de publicidad y comercialización; los servicios y transacciones financieros; el turismo; los servicios de información y distracción y los sistemas auxiliares que contribuyen a las actividades económicas y comerciales.

Entre los productos tangibles que probablemente se intercambian cada vez más por medios electrónicos cabe citar: los productos informáticos, los libros, la música, los regalos y las flores, la ropa y los productos alimentarios y agrícolas.

Vale la pena señalar que el comercio de servicios constituirá probablemente una parte más importante de la actividad del comercio electrónico que los productos digitalizados. Esta actividad ha tenido lugar en su inmensa mayoría en países con economías e infraestructura avanzadas."

Latinoamérica y el comercio electrónico: extractos del artículo "El Miedo al Fraude es el Principal Obstáculo Para el Desarrollo de Internet en América Latina" aparecido en el sitio MasterNet.com[6]

"La baja penetración de Internet y una percepción de riesgo de fraude con las tarjetas de crédito son los principales factores que frenan el despegue del comercio electrónico en América Latina."

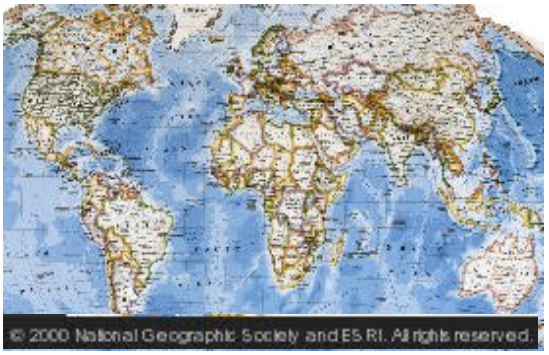
Una encuesta de la International Data Corporation (IDC) efectuada a 165 comercios "virtuales" de América Latina, afirma que el temor de los consumidores es infundado, ya que el 73% de las empresas encuestadas manifestó facilitar transacciones electrónicas seguras utilizando la misma tecnología que sus homólogos Estadounidenses. De acuerdo con los resultados arrojados en esta encuesta, la mayoría de las empresas "virtuales" de la región ofrecen a sus clientes aplicaciones de pago en línea seguras (por ejemplo: *Secure Sockets Layer* [SSL[7]]).

[6] El artículo está publicado en esta página web: http://www.masterdisseny.com/master-net/atrasadas/104.php3
[7] Para mayor información sobre SSL, visite: http://www.ssl.com/Faq.asp

La empresa a cargo de la realización de la encuesta, sostiene que existen otros factores importantes que frenan el crecimiento de las ventas en línea. Entre estos se encuentran las dificultades socioeconómicas de la región, representadas por una gran desigualdad de ingresos, una baja penetración de la tarjeta de crédito, altos costes de envío y una inadecuada infraestructura de telecomunicaciones.

No obstante los mencionados obstáculos al buen desarrollo del comercio electrónico y con una visión optimista, la IDC espera que las ventas en línea alcancen alrededor de 1.8 billones de dólares americanos durante este año y de los 11 billones de dólares americanos en el 2003. Asimismo, y de acuerdo con la información suministrada por la IDC, alrededor de 12 millones de latinoamericanos utilizan Internet. Estos consultores esperan que esta cifra sea triplicada el año entrante.

El e-business en sesenta (60) países por The Economist Intelligence Unit (EIU)/Pyramid Research e-readiness rankings - The EIU ebusiness forum. Mayo 2001.[8]



Consideramos que podría ser interesante para el lector obtener información sobre el ranking de países elaborado por *The Economist Intelligence Unit* y el *ebusiness forum*. Este ranking tiene por objeto clasificar a los países en cuatro categorías relacionadas con el nivel de desarrollo del *e-business* en cada uno de ellos.

Las categorías[9] son las siguientes:

- **Líderes (*leaders*) del *e-business*.** Países clasificados bajo esta categoría poseen la mayor parte de los elementos de "*e-readiness*", aun cuando existen ciertas reservas en la regulación y reglamentación sobre seguridad.
- **Contendientes (*contenders*) del *e-business*.** Los países incluidos en esta categoría tienen una infraestructura satisfactoria y un buen ambiente de negocios. Pero algunas ecuaciones del *e-business* siguen faltando.
- **Seguidores (*followers*) del *e-business*.** Estos países –el grupo mayoritario según el ranking del *EIU*– han comenzado a crear un ambiente propicio para el *e-business*, pero todavía tienen mucho trabajo que hacer.
- **Rezagados (*laggards*) del *e-business*.** Los países incluidos dentro de esta clasificación corren el riesgo de quedarse atrás y deberán enfrentar mayores obstáculos al crecimiento del *e-business*, principalmente, en lo que se refiere a la conectividad.

Véase a continuación, el cuadro con el ranking de nivel de *e-business* por país: (Ver página siguiente)

[8] El contenido (incluso el cuadro) del trabajo del EIU ha sido reproducido con el consentimiento del Editor en Jefe, Servicios e-business, Editor del ebusinessforum.com, obtenido mediante mensaje electrónico de fecha 12 de abril de 2002.

[9] La traducción al español de las categorías incluídas en el cuadro ha sido realizada por el autor de este trabajo de armonización de la legislación sobre comercio electrónico de los Países Miembros de la Comunidad Andina.

The Economist Intelligence Unit Pyramid Research e-readiness rankings		
E-readiness ranking (of 60)	**Country**	**E-readiness score (of 10)**
	E-business leaders	
1	US	8.73
2	Australia	8.29
3	UK	8.10
4	Canada	8.09
5	Norway	8.07
6	Sweden	7.98
7	Singapore	7.87
8	Finland	7.83
9	Denmark	7.70
10	Netherlands	7.69
11	Switzerland	7.67
12	Germany	7.51
13	Hong Kong	7.45
	E-business contenders	
14	Ireland	7.28
15	France	7.26
16 (tie)	Austria	7.22
16 (tie)	Taiwan	7.22
18	Japan	7.18
19	Belgium	7.10
20	New Zealand	7.00
21	South Korea	6.97
22	Italy	6.74
23	Israel	6.71
24	Spain	6.43
25	Portugal	6.21
	E-business followers	
26	Greece	5.85
27	Czech Republic	5.71
28	Hungary	5.49
29	Chile	5.28
30	Poland	5.05
31	Argentina	5.01
32	Slovakia	4.88
33	Malaysia	4.83
34	Mexico	4.78

35	South Africa	4.74
36	Brazil	4.64
37	Turkey	4.51
38	Colombia	4.24
39	Philippines	3.98
40 (tie)	Egypt	3.88
40 (tie)	Peru	3.88
42	Russia	3.84
43	Sri Lanka	3.82
44	Saudi Arabia	3.80
45	India	3.79
46	Thailand	3.75
47	Venezuela	3.62
	E-business laggards	
48	Bulgaria	3.38
49	China	3.36
50 (tie)	Ecuador	3.30
50 (tie)	Iran	3.30
52 (tie)	Romania	3.20
52 (tie)	Ukraine	3.20
54 (tie)	Algeria	3.16
54 (tie)	Indonesia	3.16
56	Nigeria	2.91
57	Kazakhstan	2.76
58	Vietnam	2.76
59	Azerbaijan	2.72
60	Pakistan	2.66

Fuente: The Economist Intelligence Unit/Pyramid Research e-readiness rankings

B. La Comunidad Andina (CAN): Introducción, objetivos y visita a la CAN.

Introducción. La Comunidad Andina de Naciones (CAN) es un órgano supranacional que engloba un proceso de integración sub-regional surgido a raíz de la firma del Acuerdo de Cartagena en el año de 1.969. La subregión se encuentra actualmente constituida por Bolivia, Colombia, Ecuador, Perú y Venezuela, países que en su conjunto conforman un espacio geográfico de 4.710.000 kms², en el que habitan más de 110 millones de personas.

Objetivo principal de la CAN. El objetivo principal de la comunidad es promover el desarrollo armónico y equilibrado de sus Países Miembros, mediante la integración y la cooperación económica y social; así como, disminuir la vulnerabilidad externa y mejorar la posición de los Países Miembros en el contexto económico internacional.

La Secretaría General de la CAN. La Secretaría General de la CAN es el órgano técnico y ejecutivo que se encarga de administrar el proceso de integración, velar por el interés de los compromisos comunitarios y presentar iniciativas y propuestas de Decisión.

El comercio electrónico y la CAN. El comercio electrónico ha sido objeto de múltiples debates y reuniones presididos por esa Secretaría. Algunas de las recomendaciones adoptadas en la CAN sobre este tema han sido las siguientes:

- Ejecutar un plan integral para superar las dificultades y obstáculos que impiden el desarrollo del comercio electrónico.
- Exhortar a los países de la Comunidad Andina a que aproximen su legislación sobre la materia, para su posterior armonización, contribuyendo así al establecimiento del Mercado Común[10].
- Evaluar todos y cada uno de los cuerpos jurídicos de cada país para evitar contradicciones o posteriores acciones en contra de las Leyes Marco que se implementen.
- Establecer los mecanismos e instrumentos jurídicos que brinden seguridad a las transacciones comerciales que se realizan por el medio digital.
- Lograr la consolidación del principio de equivalencia funcional del documento electrónico y firma electrónica en las leyes, para que puedan competir en igualdad de condiciones con los documentos tradicionalmente aceptados.

Actualmente, la CAN está llevando a cabo un estudio de las legislaciones vigentes sobre comercio electrónico de sus Países Miembros a fin de armonizar su contenido y proponer el texto de una Decisión comunitaria.

La UIT y ASETA visitan la CAN.

Considerando la iniciativa de ASETA de llevar a cabo un estudio de derecho comparado de las leyes sobre comercio electrónico de los Países Miembros de la Comunidad Andina, que tiene por objeto elaborar un conjunto de recomendaciones para la armonización de las mismas con asistencia de la UIT y

Considerando la tarea de la CAN de elaborar una Decisión comunitaria por medio de la cual se armonice la legislación sobre comercio electrónico de sus Países Miembros;

ASETA y la UIT se reunieron en la Secretaría de la CAN en Lima-Perú en el mes de marzo de 2002, para ofrecer el resultado del estudio que han emprendido desde el mes de enero de 2002 y que está contenido en las recomendaciones aquí expuestas.

[10] Dentro del proceso de integración, la CAN se ha fijado como principal objetivo el establecimiento de un mercado común para el año 2005. Dicha etapa de integración permitirá alcanzar la plena liberación del comercio sub-regional de bienes y de servicios, así como la libre circulación de personas y el libre flujo capitales.

C. Proyecto UIT – WISeKey de despliegue de Entidades / Autoridades de registro en el mundo

En vista de que en este documento se trata el tema de las entidades de registro y certificación, aprovechamos esta oportunidad para ofrecerles información sobre el proyecto de despliegue de entidades de registro en países en desarrollo llevado a cabo por la Unión Internacional de Telecomunicaciones.

Antecedentes cronológicos.

En 1998, fue lanzado en la Unión Internacional de Telecomunicaciones (UIT) el proyecto Comercio Electrónico para Países en Desarrollo (EC-DC) dependiente de la Oficina de Desarrollo de las Telecomunicaciones (BDT).

A fin de implementar el programa *Valleta Action Plan* (VAP) y las actividades prioritarias de la UIT Desarrollo (UIT-D) para el período 1999-2003, la BDT está trabajando conjuntamente con la industria privada en la creación de tecnologías de comercio electrónico para países en desarrollo y menos adelantados.

En mayo de 1999, la UIT firmó un contrato de asociación con WISeKey SA y la *World Trade Centre* (WTC) de Ginebra a fin de expandir el proyecto de Comercio Electrónico para Países en Desarrollo a nivel mundial, por medio del uso de los servicios de certificación y la Infraestructura de Clave Pública (PKI) de WISeKey.

Dentro del marco del proyecto EC-DC y en ejecución de los términos del acuerdo de asociación, la UIT ofrece una plataforma para que la industria privada asista a los países en desarrollo en el establecimiento de una infraestructura de *e-business*. La UIT no endosa ningún tipo de tecnología y sus acuerdos de asociación con la industria privada son neutrales y no exclusivos.

En el año 2000, se concretó la colaboración de la industria privada, a través del proyecto de despliegue de Entidades / Autoridades de Registro en todas las regiones del mundo. Asimismo, en concordancia con los términos del acuerdo de asociación, se han desarrollando aplicaciones PKI para *e-business* en beneficio de los países en desarrollo.

En mayo de 2001, la UIT y WISeKey lanzaron un portal seguro que incluye un micro mercado *business to business* (B2B) basado en tecnología PKI y anunciaron el acercamiento tecnológicamente neutro para el desarrollo de un PKI global.

Desde junio de 2001, la UIT y WISeKey expresaron estar capacitados para asegurar la emisión y entrega de certificados digitales (*Digital IDs*) en una escala global.

A partir de agosto de 2001, nuestros socios industriales comenzaron a prestar servicios y a librar productos creados para países en desarrollo y menos adelantados. Esto incluye las aplicaciones necesarias para el despliegue de Entidades / Autoridades de Registro y servicios conexos creados para emitir y usar certificados digitales de manera completamente operacional.

Tipo de asistencia.

El proyecto ofrece asistencia para crear una infraestructura confiable / fiable que preste servicios seguros de pago en línea y transacciones electrónicas seguras para países en desarrollo y menos adelantados. Además, se lleva a cabo una capacitación y formación y se transfieren nuevas tecnologías que incrementan la capacidad y el conocimiento del personal local para sostener el proyecto.

De conformidad con el acuerdo de asociación mencionado *supra*, las soluciones desarrolladas para el despliegue de Entidades / Autoridades de Registro han sido financiadas por los socios industriales de la UIT quienes para el año 2001 habían contribuido con siete millones y medio de dólares americanos en especie (7.500.000 USD).

Compañías / Organizaciones provenientes de países en desarrollo y menos adelantados están invitadas a participar en este proyecto a fin de obtener tecnología PKI a bajo costo, para establecer una infraestructura de e-business en un ambiente seguro y de confianza.

La Entidad / Autoridad de Registro.

Una Entidad / Autoridad de Registro es una entidad-red que opera jerárquicamente bajo el paraguas de una Entidad / Autoridad de Certificación. Una Entidad / Autoridad de Registro establece y verifica la identidad de personas naturales y jurídicas y solicita la emisión de un certificado digital (elemento necesario para crear confianza y seguridad en las transacciones electrónicas) a la Entidad / Autoridad de Certificación a la que se encuentra afiliada.

Introducción.

Existen cuatro niveles de infraestructura disponibles bajo la Infraestructura de Clave Pública (PKI en inglés) de WISeKey. Éstos son Bronce, Plata, Oro y Platino. Tanto los Niveles Bronce (Entidad / Autoridad de Registro Afiliada) y Plata (Entidad / Autoridad de Registro Afiliadas) prestan servicios de Entidad / Autoridad de Registro, que incluyen la identificación "cara a cara" de los solicitantes de certificados y el envío de la información autenticada que permiten a los Niveles Oro y Platino (Entidades / Autoridades de Certificación) generar, suspender, revocar, y en general, manejar el ciclo de vida de los certificados digitales.

En el modelo propuesto, los comerciantes y / o cualquier otro interesado solicitarán un certificado digital (basado en la Recomendación X.509 de la UIT) ante la Entidad / Autoridad de Registro y / o Certificación quien (basada en su tipo de servicio, ya sea, bronce, platino, oro o plata) emitirá el certificado localmente (si se trata de una Entidad / Autoridad de Certificación) o solicitará a esta última la emisión del mismo (si se trata de una Entidad / Autoridad de Registro). La Entidad / Autoridad de Registro realiza sus ganancias con la venta del certificado digital y su soporte físico.

El proyecto de la UIT llevado a cabo conjuntamente con WISeKey, se limita al llamado nivel Bronce, es decir, al despliegue de Entidades / Autoridades de Registro Afiliadas a una Entidad / Autoridad de Certificación.

Funciones de la Entidad / Autoridad de Registro Afiliada.

Las Entidades / Autoridades de Registro Afiliadas prestan servicios de Oficina de Registro a los usuarios finales. Éstas aseguran la identificación de los solicitantes de un certificado digital, el proceso de generación de certificados, las solicitudes de suspensión y revocación de éstos, así como mantener un archivo de todos estos servicios.

Las funciones principales que deben desempeñar estas Entidades / Autoridades son las siguientes:

a. ***La identificación del usuario final.*** Una de las actividades fundamentales que debe desarrollarse para prestar servicios de certificación, es la identificación de la entidad a la cual se va a emitir un certificado, ya sea esa entidad, una persona natural o jurídica. Por la facilidad de su despliegue y el bajo costo de los sistemas requeridos para la puesta en marcha de Entidades / Autoridades de Registro Afiliadas, las mismas son candidatos ideales para desempeñar directamente la identificación de los solicitantes o saber cuáles entidades locales pueden, en una forma segura, prestar tales servicios de identificación (por ejemplo: los notarios, Cámaras de Comercio, y Registros de Comercio).

   En consecuencia, la Entidad / Autoridad de Registro Afiliada puede desarrollar su propio plan de negocios para determinar si la identificación debe ser hecha directamente por ella o, si por el contrario, puede sub-contratar a una tercera entidad que cumpla con los procedimientos de alta seguridad exigidos por la Infraestructura de Clave Pública (PKI en inglés) de WISeKey descritos en la Declaración de Prácticas de Certificación (DPC) de WISeKey.

   En algunos casos, la Entidad / Autoridad de Registro Afiliada puede ser instalada en el seno de una institución o empresa a fin de asegurar la prestación de los servicios de certificación para sus

empleados. En estos casos, los procedimientos de identificación pueden ser realizados internamente ya que los registros de cada empleado ya existen y son de fácil acceso.

b. ***La generación segura del par de llaves o claves criptográficas.*** La Entidad / Autoridad de Registro Afiliada que adquiera la infraestructura necesaria para prestar servicios de certificación digital, tendrá la capacidad de generar pares de claves criptográficas conforme a los estándares internacionales garantizando que ninguna copia del par de llaves o claves generadas es conocida por terceros. El servicio Bronce suministra la implementación estándar para la generación de un par de claves altamente seguras. Esto está basado en las capacidades de un puerto USB Token dedicado y los productos de tarjeta inteligentes que generan el par de claves en el equipo mismo. La clave criptográfica privada nunca se encontrará fuera del equipo y como está protegida contra lecturas no hay manera de recuperarla, de hacer una copia de respaldo o archivarla utilizando este método.

c. ***La solicitud de expedición, renovación, suspensión y revocación de certificados***.

d. ***El mantenimiento de los archivos de sus operaciones, incluida la documentación presentada por los solicitantes de certificados.*** La Entidad / Autoridad de Registro Afiliada debe mantener un archivo de sus operaciones, que incluye los documentos físicos presentados por los solicitantes de certificados. Este archivo constituye una parte esencial del suministro de servicios de certificación porque en caso de que exista duda en la validez de un certificado o de una firma digital el procedimiento seguido por la entidad de registro y los documentos archivados serán la prueba de que el proceso de certificación fue realizado apropiadamente.

e. ***El entrenamiento local acerca de la seguridad de la información y el uso de certificados de Clave Pública.*** Muchos clientes requerirán entrenamiento en los problemas que surgen con relación a la seguridad de la información y a la utilización de los certificados de manera que haga máximo sus beneficios. Tales cursos de entrenamiento pueden ser diversificados en otras áreas relacionadas a la tecnología de la información y por lo tanto crearían ingresos adicionales para la Entidad / Autoridad de Registro Afiliada.

f. ***La distribución de los certificados, claves o códigos (PIN) y los dispositivos para el almacenaje del par de llaves o claves de sus clientes (tarjetas inteligentes, Ikey o token, etc.).*** Si la Entidad / Autoridad de Registro Afiliada decide disponer de un centro completo de proceso de certificación, tendrá la capacidad para manejar localmente la distribución de certificados, de Tokens para claves o llaves criptográficas y de tarjetas inteligentes que contengan el número de identificación personal (clave o código PIN) necesarias para la activación de los certificados. Dependiendo de la implementación requerida por la Entidad / Autoridad de Registro Afiliada, esto puede incluir la impresión de tarjetas inteligentes (por ejemplo, con el logotipo de la Entidad / Autoridad, la fotografía y / o el logotipo del cliente).

g. ***Servicios que generen ingreso adicional.*** Los certificados son una herramienta que se puede utilizar para muchos propósitos, de la misma manera que una firma manuscrita se ha utilizado durante siglos. Para satisfacer las necesidades de sus clientes, las Entidades / Autoridades de Registro Afiliadas pueden tener una amplia variedad de aplicaciones y servicios en línea a los cuales sus clientes pueden tener acceso mediante el pago de una tarifa y la compra de un certificado. En tales casos la Entidad / Autoridad de Registro Afiliada puede generar ingresos adicionales por la venta de aplicaciones o de servicios en línea.

Adicionalmente, las Entidades / Autoridades de Registro Afiliadas pueden:

a. determinar las políticas de certificación que apoyarán a aquellas políticas disponibles a través de la Entidad / Autoridad de Certificación Afiliada que emitió su certificado;

b. hacer que la Interfase de la Entidad / Autoridad de Registro Afiliada esté ajustada a las propias necesidades locales; por ejemplo: soporte en el idioma local, formato de presentación ajustado a la localidad, etc;

c. en caso de ser necesario, negociar con la Entidad / Autoridad de Certificación Afiliada que emitió el certificado, la posibilidad de adoptar sus políticas de registros de usuarios de certificados, ajustada a sus propias necesidades locales;

d. tener una infraestructura dedicada para prestar los servicios de certificación requeridos por sus Entidades / Autoridades de Registro Afiliadas y por los usuarios finales.

Requisitos necesarios para el funcionamiento de una Entidad / Autoridad de Registro Afiliada.

Para desempeñar tales funciones, las Entidades / Autoridades de Registro Afiliadas requieren cumplir con:

a. la Declaración de Prácticas de Certificación de la Entidad / Autoridad de certificación Afiliada de la cual depende;
b. las políticas de certificación correspondientes a los procesos de los certificados (por ejemplo, identificación de los certificados, confidencialidad, etc.) y las políticas de privacidad;
c. la guía de administración de la Entidad / Autoridad de Registro Afiliada;
d. el acuerdo entre la Entidad / Autoridad de Certificación Afiliada y la Entidad / Autoridad de Registro Afiliada.

Requisitos para operar una Entidad / Autoridad de Registro Afiliada

a. ***Infraestructura física*****.**

- Archivos de programas en línea.
- Archivos de seguridad para documentos físicos a prueba de fuego y agua, en línea y fuera de línea (*On-site* y *Off-site*).
- Área con acceso restringido (espacio dotado de un mecanismo de cierre razonablemente seguro y accesible sólo a personas autorizadas para trabajar en el servicio del proveedor del Servicio Nivel Bronce).
- Compartimiento seguro o caja fuerte (con un mecanismo de cierre razonablemente seguro y accesible solamente por el personal autorizado para operar el sistema) en el cual se debe guardar la tarjeta inteligente mientras el sistema de Servicio Nivel Bronce no está en uso.

b. ***Servicios tecnológicos*****.**

- Servicios local de soporte y de mantenimiento técnico del sistema.
- Conexión a un proveedor de servicio de Internet a una velocidad por lo menos 33,6 Kbps o conexión "LAN" directa a Internet.
- Suministro eléctrico.

c. ***Personal.***

- Dos (2) personas dedicadas con la habilidad para llevar a cabo chequeos y para el registro de usuarios (experiencia previa en establecer registros de empresa o práctica en registros de comercio).
- Un operador de la Entidad / Autoridad de Registro.

d. ***Documentos.*** Los siguientes documentos deben ser presentados durante la fase de presentación de requisitos para el funcionamiento de una Entidad / Autoridad de registro:

- Copia de sus estatutos debidamente registrados en el Registro de Comercio conjuntamente con la dirección física del lugar donde la Entidad / Autoridad de Registro Afiliada será ubicada, y el nombre de la persona designada por la Entidad / Autoridad como responsable de esta operación. Para aquellas organizaciones que no estén registradas en el Registro de Comercio se acepta por ejemplo documento oficial de entidades públicas, notarías, etc.
- Los nombres y un certificado judicial o policial de cada uno de los empleados relacionados con las funciones de la Entidad / Autoridad de Registro.
- Una declaración firmada por la Entidad / Autoridad que certifique la existencia de instalaciones seguras con estrictos controles de acceso (por ejemplo Seguros y llaves, acceso con tarjetas inteligentes, o biométricas, etc.), y en donde el acceso está restringido sólo al personal autorizado.
- Una descripción del mercado para los certificados digitales en el que el solicitante presuma que puede penetrar.
- Firma de un acuerdo bilateral de confidencialidad.
- Una confirmación de un proveedor reconocido de tecnología de la información acerca de la capacidad de la Entidad / Autoridad relativa a:
  - El acceso por parte de la Entidad / Autoridad a servicios locales de soporte técnico, que puedan garantizar la constante interfase con la Entidad / Autoridad de Certificación.
  - La disponibilidad en la Entidad / Autoridad de una estación de trabajo PC dedicada.
  - El acceso seguro de la Entidad / Autoridad a una conexión Internet.

e. ***Requisitos operacionales.***

- Apoyo de primer nivel a los Usuarios finales – El postulante requiere asegurar que está en capacidad de proveer un soporte de primer nivel para los usuarios finales. Este soporte incluye responder todas las preguntas generales de la Infraestructura de Clave Pública (PKI), así como resolver todos los problemas relativos al uso de los certificados digitales tanto del hardware como del software.
- Servicio de Suspensión y Revocación – Los postulantes requieren estar en capacidad de prestar servicios de suspensión y revocación de acuerdo con el *Certification Practice Statement (CPS)* de Ecommerce PKI. Deben estar en condiciones de revocar o suspender un certificado luego de la petición realizada por un usuario final hecha telefónicamente, por fax o e-mail dentro de las 12 horas seguidas o contactar al servicio de Suspensión y Revocación de WISeKey dentro de las 2 horas, luego de haberse hecho la petición.
- Venta de Accesorios – Los postulantes deben estar preparados para ofrecer el equipo básico a los usuarios finales tales como lectores de cartas inteligentes, extensiones USB, etc.

Contenido del paquete Bronce por medio del cual se crea e instala una Entidad / Autoridad de certificación.

El paquete Bronce incluye:

A. El PC de la Entidad / Autoridad de Registro previamente pre-configurado. El PC incluye:
   Sistema:
   a. Windows 2000
   b. Ethernet LAN adaptador y MODEM
   c. Teclado y ratón
   d. Monitor 15" LCD
   e. Lector de Tarjeta Inteligente para puerto serial
   f. Lector de Tarjeta Inteligente para puerto USB
   g. Administrador de Tarjeta Inteligente.

   Software:
   a. Unicert Web RAO
   b. Programa para el lector de Tarjeta inteligente y USB token
   c. Microsoft Internet Explorer (128 bit)
   d. Acrobat Reader.

B. Adicionalmente, el paquete Bronce incluye:
   a. Licencia del primer año para 300 certificados estándares
   b. Documentación técnica, operacional y legal
   c. Servicios de directorio y validación vía WISeKey's E-commerce PKI CA
   d. Entrenamiento para los operadores de la Entidad / Autoridad de Registro en Ginebra - Suiza
   e. Soporte vía e-mail
   f. Auditoría independiente (excluye viáticos y tiquetes / pasajes / boletos de avión)
   g. Mantenimiento del Hardware y software
   h. Orden de servicio para tarjetas inteligentes, lectores y tokens.

El paquete Bronce no incluye:

a. La instalación por su parte del sistema *Bronze Service Provider (BSP)* o proveedor de servicios nivel bronce.
b. La conexión a Internet u otras facilidades de comunicación
c. Los costos de comunicación.

NOTA: El sistema BSP debe ser estrictamente utilizado con el propósito de registrar usuarios de certificados y no debe ser usado para ninguna otra aplicación o propósito fuera del definido en el contrato de las Entidades / Autoridades de Registro Afiliadas.

Licencias de exportación y envío del paquete. El envío del paquete Bronce está supeditado a la autorización para la exportación de los productos restringidos incluidos en el paquete.

El procedimiento para convertirse en candidato del proyecto UIT-WISeKey de despliegue de Entidades / Autoridades de registro por el canal de la UIT.

Además de cumplir con los requisitos necesarios para funcionar y operar una Entidad / Autoridad de Registro Afiliada, la compañía / organización que desee formar parte del proyecto deberá expresar su intención ante el Ministerio de Telecomunicaciones u otra Administración del país que se encuentre en relación directa con la UIT.

Dicho Ministerio de Telecomunicaciones u otra entidad de la Administración deberá enviar una carta vía fax a la atención del:

Sr. Hamadoun I. Touré,
Director, UIT,
Oficina de Desarrollo de las Telecomunicaciones (BDT),
Place des Nations,
CH-1211 Ginebra 20 Suiza.
Telf. + 41 22 730 55 33
Fax +41 22 730 54 84

La entidad correspondiente deberá postular / recomendar a “X” compañía / organización, para que se convierta en entidad / autoridad de registro dentro del marco del proyecto UIT-WISeKey de despliegue de Entidades / Autoridades de registro para el establecimiento de transacciones electrónicas seguras.

Parte II: Estudio de Derecho comparado. Semejanzas y diferencias de la normativa de los países de la Comunidad Andina[11] y recomendaciones para su armonización.

Esta parte del trabajo está consagrada a la comparación de las disposiciones de la normativa vigente y en proyecto sobre comercio electrónico de los Países Miembros de la Comunidad Andina. Aquí identificamos cuáles son las semejanzas y diferencias entre las mismas y hacemos mención de las normas legales adoptadas de acuerdo con los lineamientos de las leyes modelo sobre comercio electrónico y firma electrónica de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL)[12], incluyendo las recomendaciones para efectos de su armonización.

Advertencia: No todos los temas abordados han sido objeto de regulación por cada uno de los países andinos. Cuando ello ocurra, el lector encontrará un mensaje similar al siguiente: "No posee disposiciones legales que traten este tema". Esto se debe a que para el momento en que se realizó la investigación objeto del presente trabajo (Dic. 2001 – Mayo 2002), no conseguimos ninguna disposición legal vigente o en proyecto que abordara cada uno de los temas tratados en el siguiente estudio de Derecho comparado y análisis.

[11] Ver cuadro comparativo en el Anexo "A" del presente trabajo.

[12] De acuerdo con la información de la CNUDMI, se han promulgado leyes basadas en su Ley Modelo sobre comercio electrónico en Australia, las Bermudas, Colombia, Eslovenia, los Estados de Jersey, Filipinas, Francia, Hong Kong, Irlanda, la República de Corea, Singapur y, dentro de los Estados Unidos de América, Illinois. Asimismo, nos informa que se ha preparado legislación uniforme influida por el modelo en cuestión y por los principios en los que ésta se basa en el Canadá y en los Estados Unidos de América y se ha promulgado en forma de Ley en diversas jurisdicciones de estos países.

A. Mensajes de datos:

1. ***Definición y ámbito de aplicación de la ley***

2. ***Definición de mensaje de datos***

3. ***Modificaciones***

4. ***Requisitos jurídicos de los Mensajes de Datos: Integridad de los Mensajes de Datos***

5. ***Requisitos jurídicos de los Mensajes de Datos: Escrito***

6. ***Requisitos jurídicos de los Mensajes de Datos: Original***

7. ***Reconocimiento jurídico de los Mensajes de Datos. Reconocimiento por parte de quien los usa***

8. ***Atribución y presunción de origen de un Mensaje de Datos***

9. ***Efectos jurídicos del Mensaje de Datos***

10. ***Incorporación por Remisión de Mensaje de Datos***

11. ***Admisibilidad y Fuerza Probatoria de los Mensajes de Datos***

12. ***Mensaje de Datos Duplicado***

13. ***Conservación de los Mensajes de Datos***

14. ***Documentos Desmaterializados***

A. Mensajes de datos:

El presente trabajo no abordará los siguientes temas: acuse de recibo del mensaje de datos, tiempo de envío y recepción del mensaje de datos y lugar de envío y recepción del mensaje de datos, ya que los mismos serán tratados en un segundo reporte que presentaremos en el segundo semestre de 2002, tal y como lo informáramos en la parte introductoria.

Igualmente, dejaremos para el segundo reporte lo relativo a las notificaciones judiciales realizadas por medios electrónicos y el análisis de la disposición peruana sobre documento electrónico en proformas o microformas.

A. Mensajes de datos:

1. Objeto y ámbito de aplicación de la Ley.

BOLIVIA - El anteproyecto de Código de Comercio regula la validez y comunicación de los mensajes de datos. El ámbito de aplicación de estos capítulos se extiende a todo tipo de información transmitida en forma de mensaje de datos.

COLOMBIA - La Ley 527[13] será aplicable a todo tipo de información en forma de mensaje de datos, (misma redacción que la adoptada en la Ley Modelo de la CNUDMI sobre comercio Electrónico[14]) salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;
b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

ECUADOR – La Ley ecuatoriana[15] regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información incluido el comercio electrónico, la protección a los usuarios de estos sistemas.

PERÚ – No posee actualmente una legislación o proyecto de ley sobre mensajes de datos. A pesar de ello, el Reglamento[16] de la Ley 27.269[17] regula la utilización de firmas electrónicas en mensajes de datos y documentos electrónicos.

VENEZUELA - El Decreto-Ley[18] 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.

El Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.

---

[13] Ley No. 527 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Fecha: 18 de agosto de 1999.

[14] UNCITRAL - Artículo 1. Ámbito de aplicación* Modelo comercio-e. La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto*** de actividades comerciales ****.
* La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales:
"La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional."
** La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.
*** La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:
"La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [...]."
**** El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje ("*factoring*"); de arrendamiento de bienes de equipo con opción de compra ("*leasing*"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

[15] Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos aprobado por el Congreso Nacional. Fecha 27 de febrero de 2002. Este proyecto de Ley fue vetado por la Presidencia de la Republica. Fecha: segunda semana de marzo de 2002. El proyecto fue finalmente aprobado en abril de 2002.

[16] Reglamento de la Ley de Firmas y Certificados Digitales Ley No. 27.269. Decreto Supremo No. 019-2002-JUS. Fecha publicación: 17 de mayo de 2002.

[17] Ley No. 27.269 de Firmas y Certificados Digitales. Fecha promulgación: 26 de mayo de 2000. Fecha publicación: 28 de mayo de 2000.

[18] Decreto-Ley No. 1024. Ley sobre Mensajes de Datos y Firmas Electrónicas. Fecha: 10 de febrero de 2001.

Semejanzas y Diferencias. Comentarios.

El Anteproyecto de Código de Comercio boliviano regula la validez y comunicación de los mensajes de datos y su aplicación se extiende a todo tipo de información transmitida en forma de mensaje de datos. Esta última declaración es muy similar a la contenida en la Ley colombiana, que está a su vez basada en los lineamientos de la Ley Modelo de la CNUDMI sobre comercio electrónico. A pesar de ello, la Ley 527, establece dos excepciones en las cuales la Ley 527 no será aplicable. La disposición venezolana que estipula tener por objeto otorgar y reconocer eficacia y valor jurídico al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, podría ser equiparada a las menciones de Bolivia y Colombia.

La reciente Ley de Comercio Electrónico del Ecuador, establece simplemente que dicha Ley regula los mensajes de datos, mientras que el Reglamento de la Ley peruana establece que regula las firmas electrónicas que aparecen en mensajes de datos. Como podremos constatar, el Reglamento establece una definición de mensajes de datos y pauta ciertas reglas en materia probatoria con respecto a aquellos mensajes que estén firmados electrónicamente.

Observamos que las disposiciones de Bolivia y Venezuela son las únicas que mencionan que sus respectivas legislaciones tratan la validez de los mensajes de datos. Sugerimos que este tipo de información se ofrezca desde un principio en las respectivas legislaciones.

Notamos que la norma venezolana es realmente innovadora, en el sentido de que se fundamenta en los principios de neutralidad tecnológica y de no-exclusividad de la tecnología al establecer que el Decreto-Ley será aplicable a los Mensajes de Datos independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro y que a tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos.

Recomendación.

Consideramos apropiado incluir este tipo de normas en una Decisión comunitaria sobre comercio electrónico que abarque los temas de mensajes de datos, firmas electrónicas (incluyendo las firmas digitales), certificados digitales y entidades de certificación; sin dejar de lado los temas que serán tratados en el segundo reporte, tales como: delitos informáticos, protección de datos (*Habeas Data)*, defensa al consumidor, derechos de autor, derecho aplicable a las transacciones electrónicas, jurisdicción y arbitraje e impuestos a las transacciones electrónicas.

A. Mensajes de datos:

2. Definición de mensaje de datos

BOLIVIA – No posee actualmente ninguna disposición legal o en proyecto.

COLOMBIA – La Ley 527 entiende por mensaje de datos, la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax. (Esta disposición está fundamentada en los lineamientos de las Leyes Modelo de la CNUDMI sobre firmas electrónicas y comercio electrónico[19], con una variante.)

ECUADOR - Para efectos de la Ley ecuatoriana, se definen los mensajes de datos como toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos. (Esta norma está fundamentada en los lineamientos de las Leyes Modelo de la CNUDMI sobre firmas electrónicas y comercio electrónico, con algunas variantes.)

PERÚ – El Reglamento de la Ley 27.269 define los mensajes de datos, como la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el Intercambio Electrónico de Datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el télex, el telefax, entre otros. (Este articulado está basado en los lineamientos de las Leyes Modelo de la CNUDMI sobre firmas electrónicas y comercio electrónico.)

VENEZUELA – A los efectos del Decreto-Ley, se entenderá por mensajes de datos, toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Semejanzas y Diferencias. Comentarios.

Es satisfactorio notar que al menos tres de los Países Miembros de la Comunidad Andina adoptaron la misma definición de mensajes de datos (con algunas variantes) consagrada en ambas Leyes Modelo de la CNUDMI.

El principio de base es el siguiente: los mensajes de datos son considerados como la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el Intercambio Electrónico de Datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el télex, el telefax, entre otros.

La Ley colombiana incluyó como parte de los mensajes de datos, a la Internet; mientras que la Ley ecuatoriana consideró los documentos y registros electrónicos y los servicios web como mensajes de datos. Pensamos que, la Internet y los Servicios Web podrían ser considerados como sinónimos o elementos equivalentes.

Las normas ecuatoriana y venezolana se asemejan en que ambas establecen que los mensajes de datos es *toda información inteligible en formato electrónico ... archivada por medios electrónicos que puede ser almacenada o intercambiada por cualquier medio*.

Recomendación.

Consideramos que una definición única y uniforme de mensaje de datos debería estar en armonía con lo dispuesto en Colombia, Ecuador y Perú.

[19] Leyes Modelo de la CNUDMI de Firmas Electrónicas y de Comercio Electrónico: Para los fines de estas Leyes: Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada 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.

A. Mensajes de datos:

3. Modificaciones

COLOMBIA – De conformidad con la Ley 527, salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones de la Parte I, Capítulo III relacionadas con la comunicación de los mensajes de datos, podrán ser modificadas mediante acuerdo. (Esta disposición se encuentra en consonancia con los lineamientos de la Ley Modelo de la CNUDCI sobre comercio electrónico[20].)

Semejanzas y Diferencias. Comentarios.

Podemos observar que el único país que tomó en consideración la voluntad de las partes y el principio general de derecho de libre contratación, es Colombia. Este país, siguiendo los lineamientos establecidos por la Ley Modelo de la CNUDCI sobre comercio electrónico, establece que la normativa sobre comercio electrónico consagrada en la Ley 527 puede ser aplicada o no, siempre y cuando medie acuerdo mutuo entre las partes que se intercambian mensajes de datos.

Recomendación.

Consideramos que esta iniciativa colombiana es plausible y debería ser tratada como un modelo a seguir en los demás Países Miembros de la Comunidad Andina.

[20] Artículo 4 de la Ley Modelo de la CNUDMI sobre comercio electrónico:

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III podrán ser modificadas mediante acuerdo.
2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes para modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el Capítulo II.

A. Mensajes de datos:

4. Requisitos jurídicos de los Mensajes de Datos: Integridad de los Mensajes de Datos

BOLIVIA – Según lo dispone el Proyecto de Código de Procedimiento Civil, se entenderá que la información es íntegra cuando haya permanecido completa e inalterada, salvo algún cambio que sea inherente al proceso de su comunicación, archivo, registro o presentación.

COLOMBIA – De acuerdo a lo pautado en la Ley 527, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

ECUADOR – De conformidad con lo previsto en la Ley ecuatoriana, se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

PERÚ – La Ley nada dice sobre la integridad de los mensajes de datos debido a que el objeto y ámbito de aplicación de la Ley recae únicamente sobre las firmas y certificados digitales. Por el contrario el Reglamento de la Ley define la integridad como la característica que indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el emisor hasta su recepción por el destinatario. El reglamento también estipula, que las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica utilizadas para firmas mensajes de datos y / o documentos electrónicos garantizan, entre otros, la integridad de los mismos y que, técnicamente la firma digital debe garantizar la integridad del mensaje de datos firmado digitalmente.

VENEZUELA – El Decreto-Ley establece que cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Semejanzas y Diferencias. Comentarios.

Podemos notar que Bolivia, Colombia, Ecuador y Venezuela adoptaron disposiciones muy similares para especificar cuándo se considera que un mensaje de datos ha conservado su integridad. Los cuatro países mencionados, establecen que la información consignada en un mensaje de datos es íntegra cuando su contenido haya permanecido completo e inalterado, salvo algún cambio que sea inherente al proceso de su comunicación, archivo o presentación.

Bolivia agrega en su disposición una cuarta excepción relacionada con los cambios inherentes al proceso de registro y Venezuela no exige que el mensaje se mantenga completo desde que se generó, solo se menciona que el mismo debe mantenerse inalterable.

Recomendación.

Opinamos que en una Decisión comunitaria debería tomarse en consideración lo establecido en las disposiciones boliviana, colombiana, ecuatoriana y venezolana, a las que hacemos referencia en la primera parte de estos comentarios, en vista del tácito acuerdo que existe en estos países para fijar las condiciones necesarias para considerar que un mensaje de datos es íntegro.

A. Mensajes de datos:

5. Requisitos jurídicos de los Mensajes de Datos: Escrito

BOLIVIA - El anteproyecto de Código de Comercio norma los actos y contratos escritos, establece los requisitos a ser cumplidos por las partes y determina cuándo la información es accesible para su ulterior consulta.

COLOMBIA - Escrito Ley 527. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito. (Esta disposición sigue al pie de la letra los lineamientos de la Ley Modelo de la CNUDMI sobre Comercio Electrónico[21])

ECUADOR - Artículo 6. Información escrita. Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta. (Esta norma sigue los lineamientos de la Ley Modelo de la CNUDMI sobre Comercio Electrónico)

La reciente Ley de Comercio Electrónico establece también que de requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) el consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y
b) el consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:
    1) su derecho u opción de recibir la información en papel o por medios no electrónicos;
    2) su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
    3) los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y
    4) los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

PERÚ - Cabe recordar, que Perú adoptó una Ley de Firmas y Certificados Digitales, motivo por el cual, no se incluyó ninguna disposición peruana dentro de este punto.

VENEZUELA - Cumplimiento de solemnidades y formalidades Decreto-Ley. Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Constancia por escrito del Mensaje de Datos Decreto-Ley. Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta. (Este artículo del Decreto-Ley se encuentra en consonancia con los lineamientos de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.)

---

[21] Artículo 6 de la Ley Modelo de la CNUDMI sobre comercio electrónico:

1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.
2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.
3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Semejanzas y Diferencias. Comentarios.

Las normas legales colombiana, ecuatoriana y venezolana, acogen plenamente los lineamientos de la Ley Modelo citada anteriormente, ya que las tres estipulan que cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Como podemos ver, la información suministrada sobre el Ante-proyecto de Código de Comercio de Bolivia no es suficiente para hacernos una idea de su contenido. Sabemos solamente que se dispone que los actos y contratos escritos pueden ser presentados en formato electrónico previo cumplimiento de ciertos requisitos y que la información contenida en los mismos, debe estar accesible para su posterior consulta, tal y como lo manifiesta la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

Observamos que Ecuador ha incluido en su Ley de Comercio Electrónico, por razones que le incumbe solamente al Legislador Ecuatoriano, disposiciones sobre defensa al consumidor. Sin perjuicio de los beneficios que esta normativa pueda aportar, consideramos que este tipo de normas debe estar contenida en las respectivas leyes de protección y defensa al consumidor existentes en todos los Países Miembros de la Comunidad Andina.

Recomendación.

Si este tema en particular es tratado en una eventual Decisión comunitaria, recomendamos que la disposición vaya en el mismo sentido que las normas colombiana, ecuatoriana y venezolana. No obstante, consideramos que toda norma relativa a la protección y defensa del consumidor debería ser tratada por separado en una Decisión comunitaria posterior.

A. Mensajes de datos:

6. Requisitos jurídicos de los Mensajes de Datos: Original

BOLIVIA – El Proyecto de Código de Procedimiento Civil estipula que cuando la ley requiera que un documento sea presentado y conservado en su forma original, este requisito queda satisfecho si se acredita que el mensaje de datos ha sido conservado íntegro a partir del momento en que se generó por primera vez y en su forma definitiva y sea accesible para su ulterior consulta.

COLOMBIA – La Ley 527 dispone que cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.
b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original. (Este artículo se corresponde plenamente con lo dispuesto en la Ley Modelo de la CNUDMI sobre comercio electrónico[22].)

ECUADOR – La Ley ecuatoriana prevé que cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

PERÚ – Para la fecha en que se realizó este trabajo, Perú no poseía normas relacionadas con este tema.

VENEZUELA – El Decreto-Ley establece que cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible.

Semejanzas y Diferencias. Comentarios.

Bolivia, Ecuador y Venezuela establecen en su normativa legal que cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si:

a. se ha conservado la integridad de su contenido. (La Ley ecuatoriana agrega que deberá comprobarse que se ha conservado la integridad del contenido del mensaje) y
b. la información contenida en dicho Mensaje de Datos esta disponible (redacción venezolana) y / o sea accesible para su posterior consulta (redacción boliviana). La Ley ecuatoriana nada dice respecto a este segundo requisito.

---

[22] Artículo 8 de la Ley Modelo de la CNUDMI sobre comercio electrónico:

1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:
   a) si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
   b) de requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.
2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.
3) Para los fines del inciso a) del párrafo 1):...
4) Lo dispuesto en el presente artículo no será aplicable a: [...].

La disposición colombiana, fidedigna al contenido de la tantas veces mencionada Ley Modelo de la CNUDMI, estipula una norma similar a la adoptada por sus países vecinos. El elemento adicional que aparece plasmado en la Ley 527 es el de "garantía". Esta Ley exige que haya una garantía confiable de que se ha conservado la integridad de la información. Asimismo, establece como requisito que la información debe ser mostrada a la persona que se deba presentar. Hubiese creado menos ambigüedades la fórmula siguiente: la información contenida en el mensaje de datos deberá estar disponible para su posterior consulta.

Recomendación.

Es nuestro deber aportar recomendaciones que faciliten la armonización de las leyes de comercio electrónico dentro de la Comunidad Andina, pero a su vez, debemos ofrecer soluciones a aquellos casos en los que las legislaciones sean vagas o poco comprensibles.

Por esta razón, consideramos pertinente aconsejar el uso de la fórmula adoptada por Bolivia, Ecuador y Venezuela en este punto.

A. Mensajes de datos:

7. Reconocimiento jurídico de los Mensajes de Datos. Reconocimiento por parte de quien los usa.

BOLIVIA – Información sobre este tema, no disponible.

COLOMBIA – No logramos obtener información sobre este tema en Colombia.

ECUADOR – La Ley de Comercio Electrónico estipula que previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes. El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento, conforme a la Ley.

Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en la Ley.

PERÚ – La Resolución 000103 de Aduanas establece como medio de comunicación entre Aduanas y los operadores de comercio exterior, proveedores y entidades, el Portal de Aduanas y los sistemas interorganizacionales basados en el intercambio electrónico de datos, con el efecto que la Ley les concede.

VENEZUELA – No posee normas que regulen este tema.

Semejanzas y Diferencias. Comentarios.

Con respecto a las normas de defensa y protección al consumidor consagradas en la Ley de Comercio Electrónico del Ecuador, consideramos que las mismas, deberían ser incluidas en la respectiva Ley de Protección y Defensa al Consumidor existente en los países de la subregión. Opinamos que es pertinente reiterar nuestra sugerencia de tratar el tema "Protección y Defensa al Consumidor" de manera separada. No consideramos prudente incluir normas al respecto en la tan esperada Decisión comunitaria que unificará la legislación de comercio electrónico de la Subregión Andina.

Recomendación.

Hemos citado en este punto, la Resolución peruana de Aduanas, debido a que la misma reconoce el uso de mensajes de datos en las relaciones entre el órgano Aduanal de ese país y los operadores, proveedores y entidades de comercio exterior. Pensamos que este articulado es muy innovador y apoya plenamente la modernización del estado y los esfuerzos de adaptar la realidad de un país a los avances tecnológicos. Sería espectacular el avance del Derecho Informático dentro de la subregión, si la futura Decisión Comunitaria que fundará las bases de una armonización de las legislaciones de comercio electrónico establece normas similares a la pautada en Perú.

A. Mensajes de datos:

8. Atribución y presunción de origen de un Mensaje de Datos

BOLIVIA – No obtuvimos información sobre este punto.

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

1. el propio iniciador;
2. por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o
3. por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o
2. el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, este último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.
El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Nota: Todo este articulado fue adoptado de conformidad con lo establecido en la Ley Modelo de Comercio Electrónico[23].

ECUADOR - Salvo prueba en contrario, de conformidad con la Ley de Comercio Electrónico, se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) si se hubiere dado aviso que el mensaje de datos no provenía de quien consta como emisor; en este caso el aviso se hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y
b) si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o se hizo caso omiso de su resultado.

---

[23] Atribución de los mensajes de datos según la Ley Modelo de Comercio Electrónico:
1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.
2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:
a) por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o
b) por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.
3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:
a) para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o
b) el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.
4) El párrafo 3) no se aplicará:
a) a partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o
b) en los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.
5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en la Ley y demás normas legales aplicables.

PERÚ – No posee normas que regulen este punto.

VENEZUELA – No posee normas que regulen este punto.

Semejanzas y Diferencias. Comentarios.

Si bien ambos países, Colombia y Ecuador, abordan los mismos temas presunción de origen o procedencia del mensaje de datos y atribución del mensaje de datos, podemos notar que Colombia detalla cada una de las posibilidades a las que el iniciador y el destinatario del mensaje de datos pueden enfrentarse; mientras que la norma ecuatoriana establece una especie de regla general.

Recomendación.

Consideramos que la materia relacionada con la presunción de origen o procedencia del mensaje de datos y atribución del mensaje de datos debe estar regida por acuerdos entre las partes (iniciador y destinatario del mensaje de datos). Ahora bien, ¿qué sucede si las partes no hacen referencia a estos temas y la ley nada dice al respecto? La legislación no podrá subsanar el vacío.

Es por esta razón que recomendamos la inclusión de una disposición en este sentido en toda Ley que abarque al comercio electrónico, a los mensajes de datos, etc. Lo mismo se aplica a una Decisión Comunitaria.

A. Mensajes de datos:

9. Efectos jurídicos del Mensaje de Datos

BOLIVIA – El Proyecto de Código de Procedimiento Civil expresa que se reconoce efectos jurídicos, validez y fuerza probatoria a los mensajes de datos, entendidos como la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o a través de cualquier otra tecnología.

COLOMBIA - No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos según lo pautado en la Ley 527. (Esta norma ha sido elaborada de conformidad con lo dispuesto en la Ley Modelo de la CNUDMI sobre comercio electrónico[24].)

Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

ECUADOR – No posee disposiciones legales que traten este tema. (Ver reconocimiento jurídico de los mensajes de datos)

PERÚ - No posee disposiciones legales que traten este tema. (Ver reconocimiento jurídico de los mensajes de datos)

VENEZUELA - Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en el Decreto-Ley.

Semejanzas y Diferencias. Comentarios.

El proyecto boliviano reconoce efectos jurídico, validez y fuerza probatoria a los mensajes de datos, mientras que la Ley colombiana manifiesta que no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos. El Decreto-Ley venezolano no fija una posición clara al respecto.

Recomendación.

El articulado colombiano fue elaborado de acuerdo con lo establecido en los lineamientos de la Ley Modelo antes citada. Consideramos que no está demás incluir esta norma en una futura Decisión comunitaria que tenga como objetivo final la armonización de las normas de comercio electrónico de los Países Signatarios del Acuerdo de Cartagena, cabe decir, Bolivia, Colombia, Ecuador, Perú y Venezuela.

Consideramos que los puntos reconocimiento y efectos jurídicos de los Mensajes de Datos deberían ser unificados en un solo tópico, para evitar confusiones.

[24] Artículo 12 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

1) En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.
2) Lo dispuesto en el presente artículo no será aplicable a: [...].

A. Mensajes de datos:

10. Incorporación por Remisión de Mensaje de Datos

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos de acuerdo a lo pautado por la Ley 527. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

ECUADOR – La Ley ecuatoriana reconoce la validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

PERÚ – No posee disposiciones legales que traten este tema.

VENEZUELA - No posee disposiciones legales que traten este tema.

Semejanzas y Diferencias. Comentarios.

El principio de la incorporación por remisión de documentos en un mensaje de datos está consagrado en la Ley Modelo de la CNUDMI sobre Comercio Electrónico[25].

Colombia y Ecuador, adoptaron dicho principio a través de la elaboración de textos relativamente similares. La norma colombiana establece "la incorporación por remisión" como una regla que puede ser modificada por acuerdo entre las partes, mientras que la norma ecuatoriana estipula como regla la necesidad imperativa de que las partes conozcan el contenido de la información "anexada" al mensaje de datos y que expresen su consentimiento en aceptarlo.

Mientras que la Ley colombiana prevé que, entre las partes y conforme a la ley, los términos incorporados por remisión serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos; la Ley ecuatoriana reconoce la validez jurídica a la información contenida indirectamente en un mensaje de datos, en forma de remisión o de anexo accesible mediante un enlace electrónico directo.

Cabe notar que la disposición colombiana es más completa, ya que cita qué tipo de información puede ser incorporada por remisión a un mensaje de datos: directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles. Además, precisa que la remisión puede ser total o parcial.

Recomendación.

Consideramos que una norma sobre la incorporación por remisión, según lo establece la Ley colombiana, no debería faltar en una Decisión comunitaria que tenga como objetivo armonizar las leyes de comercio electrónico de los Países Miembros de la Comunidad Andina.

---

[25] Artículo 5 bis de la Ley Modelo de Comercio Electrónico: No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

A. Mensajes de datos:

11. Admisibilidad y Fuerza Probatoria de los Mensajes de Datos

BOLIVIA – El Anteproyecto de Código de Comercio, reconoce valor probatorio de los mensajes de datos.

El Proyecto de Código de Procedimiento Civil, establece que los mensajes de datos son medios legales de prueba. Asimismo estipula que para valorar la fuerza probatoria de un mensaje de datos, se estimará primordialmente la fiabilidad del método por el que haya sido generado, archivado, comunicado o conservado. (Esta disposición está parcialmente basada en lo dispuesto en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, que citaremos más adelante).

COLOMBIA – La Ley 527, establece que los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original. (Esta norma está fundamentada en los principios sentados en la Ley Modelo de la CNUDMI sobre Comercio Electrónico.)

Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas, de conformidad con la Ley 527.

Por consiguiente habrán de tenerse en cuenta:

a. la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje,
b. la confiabilidad en la forma en que se haya conservado la integridad de la información,
c. la forma en la que se identifique a su iniciador y
d. cualquier otro factor pertinente.

Esta norma está fundamentada en los principios sentados en la Ley Modelo de la CNUDMI sobre Comercio Electrónico[26]

ECUADOR - Los mensajes de datos, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil (CPC).

La prueba se practicará de conformidad con lo previsto en el CPC y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados;

---

[26] Admisibilidad y fuerza probatoria de los mensajes de datos en la Ley Modelo de la CNUDMI sobre Comercio Electrónico:

1) en todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:
   a) por la sola razón de que se trate de un mensaje de datos; o
   b) por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

c) El facsímil, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta Ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la Ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

La prueba será valorada bajo los principios determinados en la Ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

PERÚ – El Reglamento de Ley 27.269, estipula que los documentos firmados electrónicamente podrán ser ofrecidos como prueba en toda clase de procesos o procedimientos.

Tratándose de documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume, que el documento fue enviado y firmado por su titular, de manera tal que identifica y vincula al firmante, y garantiza la autenticidad e integridad del mismo. Las disposiciones y presunciones del Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

VENEZUELA - Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Semejanzas y Diferencias. Comentarios.

Es reconfortante notar que todos los países, de Bolivia a Venezuela, consideran los mensajes de datos como medios de prueba, conforme al principio establecido en la Ley Modelo. Tal vez, esta afirmación les parezca muy apresurada, ya que el Perú prevé en su proyecto de reglamento a la Ley, que sólo los documentos firmados electrónicamente podrán ser ofrecidos como prueba. Si bien esto último es cierto, no es menos cierto que los documentos firmados por medios electrónicos constituyen un tipo de mensaje de datos.

Bolivia reconoce valor probatorio a los mensajes de datos; Colombia admite su fuerza probatoria; Ecuador establece que los mensajes de datos tienen valor y efectos legales y Venezuela estipula que éstos tendrán la misma eficacia probatoria que la Ley otorga a los documentos escritos. Perú nada dice al respecto.

Colombia, Ecuador y Venezuela prevén que para la valoración y efectos legales de los mensajes de datos se observará lo dispuesto en el Código de Procedimiento Civil de cada uno de estos países.

Colombia agrega además a su conjunto de normas sobre comercio electrónico que para la valoración de la fuerza probatoria de los mensajes de datos, se tendrán en cuenta reglas de derecho positivo, como la sana crítica para la apreciación de las pruebas. La Ley colombiana es la única que adoptó, para la valoración de la fuerza probatoria de los mensajes de datos, los elementos citados en la Ley Modelo de la CNUDMI.

La Ley venezolana dispone que la información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Bolivia, Colombia y Ecuador están de acuerdo en que para valorar la fuerza probatoria de un mensaje de datos, deberá estimarse la fiabilidad del método por el que el mismo haya sido generado, archivado, comunicado o conservado. Este requisito ha sido igualmente consagrado en la Ley Modelo. La norma ecuatoriana incluye algunas variantes.

Recomendación.

Recomendamos que los principios fundamentales sentados en la normativa aquí estudiada sean reflejados en una Decisión comunitaria sobre comercio electrónico. En resumen, podemos decir que es necesario que los mensajes de datos sean reconocidos como medios legales de prueba y que a los mismos se admita valor y eficacia probatorios. Todo intento de armonización de normas sobre comercio electrónico de la Subregión Andina debe regular este aspecto de los mensajes de datos.

A. Mensajes de datos:

12. Mensaje de Datos Duplicado

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado, de acuerdo a lo dispuesto en la Ley 527. (Esta disposición fue adoptada conforme a lo pautado en la Ley Modelo de la CNUDMI sobre Comercio Electrónico[27])

ECUADOR – Según lo estipula la Ley de Comercio Electrónico, cada mensaje de datos será considerado diferente y en caso de dudas las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

PERÚ – No posee disposiciones legales que traten este tema.

VENEZUELA - No posee disposiciones legales que traten este tema.

Semejanzas y Diferencias. Comentarios.

Únicamente Colombia y Ecuador adoptaron precauciones en materia de mensajes de datos duplicados. Mientras que Colombia reprodujo la disposición consagrada en la Ley Modelo citada *supra*, Ecuador se contentó con establecer que en caso de dudas las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo. Para la Ley colombiana, es deber del destinatario del mensaje actuar con la debida diligencia y / o aplicar algún método convenido para determinar si el mensaje que ha recibido es o no un mensaje duplicado.

Recomendación.

En virtud de que éste no fue uno de los temas en los que consideramos que había desacuerdo, pensamos que no es necesaria su inclusión en una Decisión comunitaria sobre comercio electrónico.

[27] Ley Modelo de la CNUDMI sobre Comercio Electrónico : El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.

A. Mensajes de datos:

13. Conservación de los Mensajes de Datos

BOLIVIA – El Proyecto de Código de Procedimiento Civil boliviano estipula que para considerar que un mensaje de datos ha sido adecuadamente conservado, será necesario que:

a. sea accesible para su ulterior consulta,
b. haya sido preservado con el formato en que se haya generado, enviado o recibido o con alguno que acredite que la reproduce con exactitud, y
c. preserve todo dato que permita determinar su origen, destino, así como la fecha y hora de su envío y recepción.

COLOMBIA – Cuando la Ley 527 requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. que la información que contengan sea accesible para su posterior consulta,
2. que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos. Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

La Ley 527, prevé que el cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

ECUADOR - Toda información sometida a esta Ley podrá ser conservada, este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a. que la información que contenga sea accesible para su posterior consulta;
b. que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c. que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido o archivado; y,
d. que se garantice su integridad por el tiempo que establezcan las normas pertinentes.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

Para aquella información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de los literales anteriores.

PERÚ – El Proyecto de Reglamento de la Ley 27.269 establece que cuando el usuario lo solicite o cuando la legislación exija que los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensajes de datos o documentos electrónicos firmados electrónicamente, deberá cumplirse con lo siguiente:

a) que sean accesibles para su posterior consulta.
b) Que sean conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido digital o electrónico.
c) Que sea conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción, en concordancia con lo establecido en el Decreto Legislativo No. 681 y sus normas complementarias.

VENEZUELA - Cuando el Decreto-Ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguientes condiciones:

a. que la información que contengan pueda ser consultada posteriormente;
b. que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida;
c. 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 en este artículo.

La Ley de licitaciones (Decreto Nº 1.121) estipula que el Ejecutivo Nacional podrá reglamentar el empleo y reconocimiento, del registro y almacenamiento de documentos en medios electrónicos y transacciones electrónicas y actos por medios telemáticos, así como otros mecanismos similares, siempre que se garanticen la transparencia, autenticidad, seguridad jurídica y confidencialidad necesaria.

Semejanzas y Diferencias. Comentarios.

Observamos con agrado que las legislaciones de los cinco países antes citados son muy similares entre sí y todas fueron adoptadas tomando como fundamento los lineamientos de la Ley Modelo de la CNUDMI sobre comercio electrónico[28]

De acuerdo con lo establecido en estos países, las condiciones necesarias para que se cumplan los requisitos de conservación de mensajes de datos son las siguientes:

a. que la información que contengan sea accesible para su posterior consulta,
b. que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
c. que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

Las variantes son las que se mencionan a continuación:

a. Ecuador previó una condición adicional: que se garantice la *integridad* del mensaje de datos por el tiempo que establezcan las normas pertinentes.
b. Perú agregó además como condición: que los mensajes de datos sean conservados con su formato original u otro formato que reproduzca en forma demostrable la *integridad* del documento electrónico, en concordancia con la legislación de la materia.

Ambos países, al adoptar tales disposiciones, tuvieron la intención de resguardar la integridad de los mensajes de datos.

Notarán, que hemos incluido en el presente punto una cita a la Ley de Licitaciones venezolana, ya que la misma estipula que el Ejecutivo Nacional podrá reglamentar el empleo y reconocimiento del "*almacenamiento*" de medios electrónicos, transacciones electrónicas, etc. De conformidad con el Diccionario de la Real Academia Española, *almacenar* significa registrar información en la memoria de un

[28] Artículo 10 de la Ley Modelo de la CNUDMI sobre comercio electrónico:

1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:
   a) que la información que contengan sea accesible para su ulterior consulta; y
   b) que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y
   c) que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.
2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.
3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1).

ordenador (Def. Informática). Pensamos que el verbo *almacenar* es, entonces, sinónimo de "*conservar*" y es en virtud de ello que hemos clasificado esta disposición de la Ley de Licitaciones bajo este punto.

Recomendación.

Consideramos que la disposición a adoptar sobre conservación de los mensajes de datos, debe acercarse más a la normativa acogida por los países, sin incluir las variantes que hemos explicado en esta parte del trabajo.

A. Mensajes de datos:

14. Documentos Desmaterializados.

ECUADOR - Por acuerdo entre las partes y cumpliendo con todas las obligaciones previstas en la Ley, se podrán desmaterializar[29] los documentos que por ley deban ser instrumentados físicamente. La Ley ecuatoriana igualmente dispone que los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades de certificación autorizadas y deberán ser conservados conforme a lo establecido en dicha Ley.

Semejanzas y Diferencias. Comentarios.

Podemos observar, que solo el Ecuador ha adoptado una norma relativa a la desmaterialización de documentos, es decir, a la posibilidad de transformar información contenida en papel en mensaje de datos o documento electrónico. Asimismo, esta norma establece que todos los documentos que por Ley sean requeridos en papel, podrán ser presentados en formato electrónico, luego de su debida transformación.

De la lectura de esta disposición se desprende que, no puede negarse valor y efectos jurídicos a los documentos en papel desmaterializados y, por ende, convertidos en documentos electrónicos que posean la correspondiente firma electrónica generada con un certificado digital emitido por una entidad de certificación de información autorizada y que hayan sido conservados de conformidad con lo pautado en la Ley.

Recomendación.

Opinamos que todos los Países Miembros de la Comunidad Andina deberían albergar en su normativa legal, una disposición que vaya en este sentido y una futura Decisión comunitaria elaborada para armonizar la legislación sobre comercio electrónico de la subregión debería, igualmente, acoger este tipo de disposiciones que beneficiarán las transacciones comerciales comunitarias.

[29] El Glosario de la Ley ecuatoriana nos informa que la desmaterialización electrónica de documentos no es más que la transformación a mensajes de datos de la información contenida en documentos físicos.

B. Firmas Electrónicas (incluyendo firmas digitales):

1. ***Objeto y ámbito de aplicación de la Ley / Proyecto de Ley o Reglamento***

2. ***Definición***

3. ***Atributos jurídicos de una Firma Electrónica y/o Digital***

4. ***Requisitos y Características de la Firma Electrónica***

5. ***Duración de una Firma Electrónica***

6. ***Extinción de la Firma Electrónica***

7. ***Invalidez de una Firma Electrónica y/o Digital***

8. ***Obligaciones del Titular de una Firma Electrónica y/o Digital***

B. Firmas Electrónicas (incluyendo firmas digitales):

Antes de empezar a esbozar las semejanzas y diferencias, consideramos pertinente hacer mención de lo que se entiende por firma electrónica y firma digital, para evitar confusiones conceptuales y percibir con mayor claridad el contenido de las disposiciones legales que trataremos más adelante. Para ello, hemos seleccionado las definiciones desarrolladas por Ysella Arguedas, Analista Legal del Instituto Peruano de Comercio Electrónico (IPCE), que citamos a continuación:

La firma electrónica "es un término genérico frente al de firma digital. Mientras la primera implica simple conformidad, la segunda va más allá, logra vincular al titular con el mensaje indubitablemente. La firma electrónica no necesariamente otorga la seguridad que da la firma digital, porque no está respaldada por el Sistema de Certificación de las Entidades de Certificación, Registro y Depósito... No existe una tercera parte involucrada en la transacción que de fe sobre el uso debido y la vigencia de la firma digital (de acuerdo al certificado respectivo).

La firma digital es, por excelencia, el instrumento de la seguridad en las transacciones electrónicas. Tiene ventajas innegables frente a la firma electrónica: permite determinar, de forma fiable, la identidad de las partes que intervienen en las transacciones, y también si el contenido del contrato celebrado fue alterado de alguna forma, posteriormente, a la aplicación de la firma.

La firma digital, en sí misma, es difícil de conceptuar, se le suele definir a través de sus elementos, sus características y la forma como se usa, debido a que en realidad es un procedimiento, una aplicación ... La firma digital es la transformación de un mensaje en un texto incomprensible, mediante la utilización de las claves pública y privada (cifrado asimétrico) ... La firma digital no puede existir independiente de un certificado digital que lo contenga, porque la firma, entendida como un conjunto de datos, es una característica del certificado."

Hecha esta referencia, pasemos a analizar el contenido de las normas jurídicas sobre comercio electrónico vigentes (o anteproyectos de Ley en curso) en Bolivia, Colombia, Ecuador, Perú y Venezuela.

Antes de entrar a comparar los textos de estos países, consideramos pertinente y necesario, hacer cita de dos disposiciones que forman parte integrante de los principios establecidos en el Reglamento de la Ley de Firmas y Certificados digitales del Perú. El principio al cual nos referimos es el de la autonomía de la voluntad de las partes, principio general de derecho que goza de reconocimiento internacional, que reposa en el texto del reciente, aprobado y publicado, Reglamento de la Ley 27.269 peruana: "Las disposiciones contenidas en el Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial de Firmas Electrónicas." A esta norma se aúna la disposición sexta de dicho Reglamento, que reza: " Para efectos de la manifestación de voluntad[30], las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos o a un documento electrónico y generadas fuera de la Infraestructura Oficial de Firma Electrónica tendrán la misma validez y eficacia jurídica que las firmas manuscritas, ..." Nótese, que estos artículos comprenden también el principio de neutralidad tecnológica.

Hacemos referencia a estas disposiciones, pues opinamos que el principio de autonomía de la voluntad de las partes juega un rol principal en el uso y reconocimiento de firmas electrónicas y certificados digitales. Debe respetarse el derecho de las partes a acordar libremente el uso de firmas electrónicas en documentos electrónicos y / o mensajes de datos, independientemente de la tecnología utilizada para generar aquellas. Obviamente, que cuando surja un conflicto entre las partes relacionado con el uso de las mismas, corresponderá a un perito especialista comprobar la eficacia de dichas firmas electrónicas generadas por

[30] Artículo 141 de la Ley 27291 que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de la voluntad y la utilización de firmas electrónicas: La manifestación de voluntad puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo. Es tácita cuando la voluntad se infiere indubitablemente de una actitud o de circunstancias de comportamiento que revelan su existencia.
No puede considerarse que existe manifestación tácita cuando la ley exige declaración expresa o cuando el agente formula reserva o declaración en contrario.

medios distintos a los generalmente reconocidos y demostrar que éstas cumplen con la misma función, vale decir, garantizar la integridad y autenticidad del contenido de un mensaje de datos o de un documento electrónico e identificar al emisor de éstos.

Perú no es el único país que recogió estos principios en su normativa legal. A tal efecto citaremos a continuación, otras disposiciones legales adoptadas por Ecuador, Perú y Venezuela sobre la tecnología.

> **ECUADOR -** La Ley ecuatoriana, reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor. Aparte de la norma mencionada anteriormente, La Ley ecuatoriana prevé que no se admitirá ninguna exclusión, restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en dicha Ley y su reglamento.

Este artículo refleja el reconocimiento tácito del principio de autonomía de la voluntad de las partes con respecto a la escogencia y uso de la tecnología que regirá su relación comercial, como también el principio de neutralidad tecnológica ampliamente reconocido por la comunidad internacional en materia de firmas electrónicas, certificados digitales y servicios de certificación digitales prestados por entidades de certificación y registro.

> **PERÚ -** El Reglamento aprobado recientemente en Perú define la Neutralidad Tecnológica como el PRINCIPIO QUE FOMENTA LA CREACIÓN Y USO DE DIVERSAS TECNOLOGÍAS, SIN PREFERIR, RESTRINGIR, NI DISCRIMINAR A NINGUNA DE ELLAS y establece que, la autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente Ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación. Asimismo estipula que, la Infraestructura Oficial de Firma Electrónica se puede basar en la siguiente tecnología de firmas electrónicas: a) Tecnología de firmas digitales, sobre la cual se basa la Infraestructura Oficial de Firma Digital y sobre b) Otras tecnologías de firmas electrónicas que sean aprobadas por la autoridad administrativa competente de acuerdo con el principio de neutralidad tecnológica. A su vez pauta que, la autoridad administrativa competente determinará los estándares compatibles aplicando el principio de neutralidad tecnológica y aprobará la utilización de otras tecnologías de firmas electrónicas distintas a las firmas digitales.
>
> **VENEZUELA -** El Decreto-Ley se aplica a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas.

Afortunadamente, tres de los cinco países de la subregión han recogido el principio de la neutralidad tecnológica y la no-exclusión de tecnología, dos de los cuales, consagran dentro de sus normas, el principio general de derecho sobre autonomía de la voluntad de las partes.

Una Decisión comunitaria sobre comercio electrónico que carezca de este tipo de principios básicos será una Decisión incompleta.

B. Firmas Electrónicas (incluyendo firmas digitales):

1. *Objeto y Ámbito de Aplicación de la Ley / Proyecto de Ley o Reglamento.*

BOLIVIA - Vista la falta de información sobre lo que sucede en Bolivia, lo único que hemos podido saber sobre la firma electrónica en este país es que el anteproyecto de Código de Comercio Boliviano admite la firma electrónica. Lamentablemente, desconocemos el alcance y sentido del verbo "admitir" empleado en el anteproyecto.

COLOMBIA - La Ley 527, siguiendo la recomendación de la Ley Modelo sobre comercio electrónico de la UNCITRAL, establece que la Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo dos excepciones.

ECUADOR - La Ley sobre comercio electrónico manifiesta de manera expresa la regulación de la firma electrónica.

PERÚ - La Ley 27.269 tiene por objeto regular la utilización de la firma electrónica que, puesta sobre un mensaje de datos o añadida o asociada lógicamente al mismo, pueda vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos. El Reglamento de la Ley peruana regula, para los sectores público y privado, la utilización de firmas electrónicas en mensajes de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica. Cualquier otra firma electrónica podrá tener los mismos efectos que los de las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, siempre que la autoridad administrativa competente apruebe su utilización.

VENEZUELA - El Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, atribuible a personas naturales o jurídicas, públicas o privadas, independientemente de su soporte material y de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de las Firmas Electrónicas.

Semejanzas y diferencias. Comentarios.

Todos los textos legales, a excepción de la Ley Colombiana, establecen la regulación de las firmas electrónicas desde un principio.

Recomendación.

Consideramos que las disposiciones de Perú y Venezuela son las más completas y acertadas, debido a que estipulan la regulación de firmas electrónicas generadas de diferentes formas (utilizando diferente tecnología) e independientemente de su soporte material. Opinamos que al momento de adoptar una legislación sobre comercio electrónico, deben regularse TODOS los tipos de firma electrónica, de conformidad con el principio internacional de neutralidad y no-exclusividad tecnológica. La disposición venezolana es innovadora, ya que establece desde un principio la intención del legislador de otorgar y reconocer eficacia y valor jurídico y probatorio a la firma electrónica. Esta opinión se aplica al contenido objeto de una futura Decisión Comunitaria sobre comercio electrónico.

B. Firmas Electrónicas (incluyendo firmas digitales):

2. *Definición.*

BOLIVIA - El proyecto de Código Tributario entiende la firma electrónica como el código numérico o alfanumérico que con carácter único, individual y reservado asigne la Administración Tributaria a cada obligado tributario. Lamentablemente, desconocemos otras definiciones de firma electrónica que hayan podido acogerse en otros anteproyectos de Ley.

COLOMBIA - La Ley 527 define a la **f**irma digital como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

ECUADOR - El Proyecto Ecuatoriano, siguiendo los lineamientos de la Ley Modelo sobre firmas electrónicas de la UNCITRAL, considera a la firma electrónica como los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

PERÚ - La Ley 27.269 entiende por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. La Ley 27.269, además, establece que la firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. El Reglamento de la Ley 27.269 indica que para efectos de ese Reglamento, se entiende por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita. Asimismo, establece que la firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido.

VENEZUELA - A los efectos del Decreto-Ley, se entenderá por firma electrónica a la información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado. Signatario es la persona titular de una Firma Electrónica.

Semejanzas y Diferencias. Comentarios.

La firma electrónica ha sido definida dentro de las disposiciones originadas en Bolivia, Ecuador y Venezuela; mientras que la firma digital fue objeto de definición por parte de las disposiciones originadas en Colombia y Perú. Solo la legislación peruana (inclusive el proyecto de reglamento a la Ley) establece ambas definiciones, es decir, las definiciones de firmas electrónicas y digitales, dejando expresamente estipulado que la segunda es un tipo de firma electrónica.

Recomendación.

Consideramos que las definiciones de firma digital colombiana y peruana, podrían ser consideradas, como modelos de disposición legal a ser acogidos por otros países. Opinamos que la definición de firma electrónica adoptada en Ecuador y en Perú, son referencias a ser tomadas en consideración al momento de redactar una norma única y uniforme que regirá en los Países Miembros de la Comunidad Andina.

Es importante recordar, que con miras a la armonización de la normativa sobre comercio electrónico de los Países Miembros de la Comunidad Andina debe, primeramente, existir un consenso en lo que se refiere a conceptos y definiciones fundamento del trabajo de armonización. Los cinco países integrantes de la subregión deben basarse en los mismos conceptos y definiciones de lo que se considera como firma electrónica, firma digital, certificado digital, entidad / autoridad de certificación, mensaje de datos, por mencionar algunos.

B. Firmas Electrónicas (incluyendo firmas digitales):

3. *Atributos Jurídicos de una Firma Electrónica y/o Digital*

BOLIVIA - El proyecto de Código Tributario estipula que con la presentación ante la Administración Tributaria de datos o información realizados vía medios magnéticos o electrónicos y firmados electrónicamente, la firma surtirá los mismos efectos legales que la firma manuscrita o autógrafa.

COLOMBIA - La Ley 527 establece que cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquélla tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo. Asimismo, estipula que el uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla cumple con ciertos requisitos determinados en la Ley.

Adicionalmente, conforme al Decreto 1.747[31], cuando quiera que un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital en la Ley 527 de 1999, sí:

a. El certificado fue emitido por una entidad de certificación abierta autorizada[32] para ello por la Superintendencia de Industria y Comercio.
b. Dicha firma se puede verificar con la clave pública que se encuentra en el certificado con relación a firmas digitales, emitido por la entidad de certificación.
c. La firma fue emitida dentro del tiempo de validez del certificado, sin que éste haya sido revocado.
d. El mensaje de datos firmado se encuentra dentro de los usos aceptados en la Declaración de Prácticas de Certificación (DPC), de acuerdo al tipo de certificado.

ECUADOR - El Proyecto Ecuatoriano establece que la firma electrónica debe tener el objeto de identificar al titular de la firma en relación con el mensaje de datos y de indicar que dicha persona aprueba y reconoce el contenido del mensaje de datos. En virtud de este atributo de la firma electrónica, el titular deberá en consecuencia, cumplir con los deberes y obligaciones derivados del contenido del mensaje de datos que haya enviado adjuntando una firma electrónica. Además, considera que la firma tiene la misma validez y efectos jurídicos que una firma manuscrita en relación con los datos consignados en documentos escritos y que la misma será considerada como medio de prueba admisible ante un juicio.

PERÚ - La Ley 27.269 otorga a la firma electrónica la misma validez y eficacia jurídica que se atribuye al uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, siempre que vinculen e identifiquen al firmante y garanticen la autenticación e integridad de los documentos electrónicos. Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos y generada bajo la Infraestructura Oficial de Firma Electrónica cumple con estas características. El Reglamento de la Ley 27.269 pauta que desde el punto de vista técnico, la firma digital debe garantizar: a) que el mensaje de datos fuera firmado con la clave privada del titular de la firma digital; b) la integridad del mensaje de datos firmado digitalmente, dado que cualquier alteración en el mensaje de datos o en la firma digital puede ser detectada; y c) que el titular de la firma digital no pueda repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada, dado que ésta se mantiene bajo su control exclusivo.

VENEZUELA - El Decreto-Ley considera que la Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. Para ello, y salvo acuerdo en contrario, la Firma Electrónica deberá garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad; ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento; y no alterar la integridad del Mensaje de Datos.

---

[31] Decreto No. 1.747 por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Fecha: del 11 de septiembre de 2000.

[32] Consideramos pertinente llamar la atención del lector en lo que se refiere al Decreto 1747 Colombiano, letra "a", ya que el mismo establece que solo las firmas electrónicas generadas por certificados digitales emitidos por entidades de certificación abiertas autorizadas tienen plena validez y eficacia jurídica. En virtud de que una decisión comunitaria debe ante todo eliminar los obstáculos al buen desarrollo y desenvolvimiento del comercio electrónico regional andino y conjugar la voluntad de sus Países Miembros, consideramos que normas de esta naturaleza deben ser evitadas dentro del marco supranacional andino.

Semejanzas y Diferencias. Comentarios.

Únicamente la Ley 527 Colombiana establece los atributos jurídicos de una firma digital, el resto de los países objeto del presente trabajo, rigen lo relacionado con los atributos jurídicos de una firma electrónica. Cabe recordar, que la firma electrónica es el género y la firma digital es la especie, ya que la misma no es más que un tipo de firma electrónica. Independientemente, de este hecho, no podemos negar que existe CONSENSO en todas estas normas nacionales (anteproyectos o leyes vigentes) para atribuir a la firma electrónica la misma validez y efectos jurídicos de la firma autógrafa o manuscrita. Nótese, que para los fines estrictos de armonización, debería adoptarse un solo concepto de firma tradicional, ya sea, firma "manuscrita" o firma "autógrafa".

Recomendación.

Tanto Ecuador como Venezuela, pautan la validez probatoria de la firma electrónica. Éste es un punto, que debe quedar claramente establecido en el proyecto de Decisión que tenga como objetivo final armonizar las normas legales sobre comercio electrónico de los Países Miembros de la Subregión Andina. Las disposiciones ecuatoriana, peruana y venezolana son muy similares. Podría elaborarse una única norma fundada en estas tres últimas disposiciones.

B. Firmas Electrónicas (incluyendo firmas digitales):

4. *Requisitos y Características de la Firma Electrónica*

BOLIVIA – Actualmente no disponemos de información suficiente para determinar si en el proceso de reforma de Bolivia habrá alguna disposición relacionada con los requisitos y características de las firmas electrónicas.

COLOMBIA - La Ley 527 estipula que el uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla cumple con los siguientes requisitos:

a) es única[33] a la persona que la usa;
b) es susceptible de ser verificada;
c) está bajo el control exclusivo de la persona que la usa;
d) está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada; y
e) está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

ECUADOR - El Proyecto Ecuatoriano estipula que para que la firma electrónica sea válida debe cumplir con los siguientes requisitos, salvo acuerdo en contrario:

a) ser individual, estar vinculada exclusivamente a su titular;
b) permite verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;
c) que el método de creación y verificación sea confiable, seguro e inalterable para el propósito por el cual el mensaje fue generado o comunicado;
d) que al momento de creación de la firma electrónica los datos con los que se creare, se hallen bajo control exclusivo del signatario;
e) que la firma sea controlada por la persona a quien pertenece y usa;
f) la firma electrónica debe estar fijada en un mensaje de datos y debe ser enviada en un mismo acto como parte integrante de aquel.

PERÚ - El Reglamento de la Ley Peruana indica que las características mínimas de la firma digital generadas bajo la Infraestructura Oficial de Firma Digital son:

a) Se genera al cifrar el código de verificación de un mensaje de datos usando la clave privada del titular del certificado digital.
b) Es única al titular de la firma digital y a cada mensaje de datos firmado por éste.
c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.
d) Su generación está bajo el control exclusivo del titular de la firma digital.
e) Está añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la firma digital o el mensaje de datos ha sido alterado.

VENEZUELA - El Decreto-Ley indica que la Firma Electrónica podrá:

a) formar parte integrante del Mensaje de Datos, o
b) estar inequívocamente asociada a éste, o
c) enviarse o no en un mismo acto.

Semejanzas y Diferencias. Comentarios.

De la lectura de las disposiciones adoptadas por las legislaciones colombiana, ecuatoriana (Proyecto de Ley), peruana y venezolana, podemos constatar que el Decreto-Ley Venezolano no estipula realmente lo que son los requisitos y características de una firma electrónica, como lo entienden los otros países. Ecuador y Venezuela se refieren a firmas electrónicas, mientras que Colombia y Perú, se refieren a firmas digitales. Consideramos que estas discrepancias que aparecen constantemente en la normativa objeto de nuestro

[33] Decreto 1747. Unicidad de la firma digital. "No obstante lo previsto en el artículo anterior, una firma digital en un mensaje de datos deja de ser única a la persona que la usa si, estando bajo su control exclusivo, dada la condición del numeral 3 del parágrafo del artículo 28 de la Ley 527 de 1999, la probabilidad de derivar la clave privada, a partir de la clave pública, no es o deja de ser remota. Para establecer si la probabilidad es remota se tendrán en cuenta la utilización del máximo recurso computacional disponible al momento de calcular la probabilidad, durante un período igual al que transcurre entre el momento en que se crean el par de claves y aquel en que el documento firmado deja de ser idóneo para generar obligaciones."

estudio, deben ser subsanadas. Una Decisión comunitaria debería tomar la iniciativa de regular las firmas electrónicas, y subsidiariamente, las firmas digitales.

Podemos constatar que HAY CONSENSO en Colombia, Ecuador y Perú sobre cuatro (04) de las características mínimas de la firma electrónica (y firma digital). La firma electrónica debe tener las siguientes características:

a) ser única al Titular;
b) ser susceptible de verificación;
c) estar bajo el control exclusivo de su Titular o Signatario*; y
d) estar asociada al mensaje de datos. (Inclusive Venezuela ha adoptado esta última como característica de la firma electrónica)

*Debemos insistir en la necesidad de uniformizar los conceptos y definiciones empleados en una Decisión comunitaria. Hemos observado que cada país tiene una manera diferente de identificar al Titular o Signatario o Suscriptor de un mensaje de datos.

Recomendación.

Consideramos que deberían retomarse las redacciones colombiana, ecuatoriana y peruana a fin de elaborar una nueva disposición que contribuirá a la armonización de las normas legales sobre comercio electrónico. Las mismas podrían combinarse para obtener resultados óptimos.

B. Firmas Electrónicas (incluyendo firmas digitales):

5. *Duración de una Firma Electrónica*

ECUADOR - El Proyecto Ecuatoriano dispone que la firma electrónica tiene una duración indefinida y podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el Reglamento a la Ley señale.

Semejanzas y Diferencias. Comentarios.

Colombia, Perú y Venezuela nada pautan sobre la duración de una firma electrónica. Desconocemos lo estipulado en Bolivia, pero presumimos que nada han estipulado al respecto.

Recomendación.

Consideramos que no es indispensable incluir esta disposición en un proyecto de Decisión de armonización de la legislación sobre comercio electrónico de los Países Miembros de la Comunidad Andina. Creemos que es suficiente estipular las causales de revocación o cancelación y suspensión temporal de la firma electrónica para que se tenga una idea de la duración de la firma electrónica. Pensamos que lo que sí se debe estipular es la duración del certificado digital en el cual reposa la firma electrónica.

Ysella Arguedas, Analista Legal del IPCE, nos explica en su artículo, que "La firma digital debe tener un período de vigencia para su utilización. Se entiende que la entidad de certificación que maneja los datos ha verificado éstos y existe un tiempo por el cual puede afirmar su certeza y veracidad con respecto a los hechos … El término prescripción implica que el derecho subsiste, pero quien es titular de él pierde la acción procesal. Es decir su derecho se vuelve inejecutable, carece de protección jurídica frente a los tribunales….Los documentos y / o firmas deben ser manejados de tal modo que: No puedan ser manipulados después de su … término de vigencia".

B. Firmas Electrónicas (incluyendo firmas digitales):

6. Extinción de la Firma Electrónica

ECUADOR - El Proyecto Ecuatoriano establece que la firma electrónica puede extinguirse por las causales siguientes: por voluntad de su titular; por fallecimiento o incapacidad de la persona natural; por disolución o liquidación de la persona jurídica, o por cualquier otra causa legal o judicialmente declarada. La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Semejanzas y Diferencias. Comentarios.

Colombia, Perú y Venezuela nada establecen sobre la extinción de una firma electrónica. Desconocemos lo estipulado en Bolivia, pero presumimos que nada han estipulado al respecto.

Recomendación.

Consideramos que este tema forma parte de lo que es la revocación o cancelación y suspensión temporal del certificado digital que genera la firma electrónica, como lo hemos mencionado previamente.

B. Firmas Electrónicas (incluyendo firmas digitales):

7. *Invalidez de una Firma Electrónica y/o Digital*

PERÚ - El Reglamento de Ley Peruana establece que una firma digital generada bajo la Infraestructura Oficial de Firma Digital pierde validez si es utilizada: a) en fines distintos para el que fue extendido el certificado digital y b) cuando el certificado haya sido cancelado.

Semejanzas y Diferencias. Comentarios.

Colombia, Ecuador y Venezuela nada establecen sobre la invalidez de una firma electrónica. Desconocemos lo estipulado en Bolivia, pero presumimos que nada han estipulado al respecto. Consideramos que este tema forma parte de los que es la revocación o cancelación y la suspensión temporal de un certificado digital generador de la firma electrónica.

Asimismo, el Proyecto de Reglamento a la Ley había previsto la invalidez de la firma digital si la misma era utilizada en operaciones que superen el valor por el cual fue autorizado, lo cual fue excluido de la redacción final del Reglamento.

Recomendación.

No obstante, recomendamos que en la normativa comunitaria que rija al comercio electrónico, sea incluido este tipo de norma como parte integrante del contenido del certificado digital y "Las limitaciones o restricciones para los usos del certificado", tal y como se establece en la Ley Ecuatoriana, ya que el elemento "valor" forma parte de los límites del certificado y en consecuencia, de la firma electrónica generada a partir de aquel.

B. Firmas Electrónicas (incluyendo firmas digitales):

8. *Obligaciones del Titular de una Firma Electrónica y/o Digital*

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - Según la Ley 527, son deberes de los suscriptores de una firma digital:

b) Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.
c) Suministrar la información que requiera la entidad de certificación.
d) Mantener el control de la firma digital.
e) Solicitar oportunamente la revocación de los certificados.

ECUADOR - Según el proyecto ecuatoriano, el titular de la firma electrónica deberá:

a) cumplir con las obligaciones derivadas del uso de la firma electrónica;
b) actuar con la debida diligencia y tomar las medidas de seguridad necesarias para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c) notificar a los interesados por cualquier medio, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y pudiere ser utilizada indebidamente;
d) verificar la exactitud de sus declaraciones;
e) responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
f) notificar a la entidad de certificación de información los riesgos sobre su firma, si cuenta con un certificado de firma electrónica, y solicitar oportunamente la cancelación de los certificados; y
g) las demás señaladas en la Ley y sus reglamentos.

PERÚ - La Ley 27.269 indica que el titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos. El Reglamento de la Ley Peruana pauta que el titular de firma digital es la persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado digital a partir del cual se generan dichas firmas digitales.

La Ley 27.269 estipula que el titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas. El Reglamento de la Ley Peruana establece que dentro de la Infraestructura Oficial de Firma Digital, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado digital. Tratándose de personas naturales, éstas son titulares del certificado y de las firmas digitales que se generen a partir de aquél, incluyendo las firmas digitales que genere a través de agentes automatizados. En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes los titulares de la firma digital, con excepción de las firmas digitales que se generen a través de agentes automatizados, situación en la cual las personas jurídicas son titulares del certificado y las firmas digitales generadas a partir de éstos. De acuerdo con lo pautado en el Reglamento, las obligaciones del titular de la firma digital son:

a. entregar información veraz bajo su responsabilidad;
b. generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la entidad de certificación;
c. mantener el control y la reserva de la clave privada bajo su responsabilidad; y
d. observar las condiciones establecidas por la entidad de certificación para la utilización del certificado digital y la generación de firmas digitales.

VENEZUELA - De acuerdo al Decreto-Ley, el Signatario de la Firma Electrónica tendrá las siguientes obligaciones:

a. Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica. (Esta obligación se encuentra en consonancia con la Ley Modelo sobre Firmas Electrónicas de la CNUDMI[34].)

[34] Proceder del firmante según la Ley Modelo de firmas electrónicas de la CNUDMI:

b. Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello. (Esta obligación se encuentra en consonancia con la norma de la Ley Modelo sobre Firmas Electrónicas de la CNUDMI.)
c. El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

Semejanzas y Diferencias. Comentarios.
Podemos constatar que hay un CONSENSO PARCIAL en lo que respecta a las obligaciones del titular de la firma electrónica. Colombia, Ecuador, Perú y Venezuela están de acuerdo en considerar que son obligaciones del titular de la firma electrónica:

a) mantener el control de la firma electrónica (y digital). (Colombia, Ecuador y Perú);
b) solicitar oportunamente la revocación o cancelación de los certificados. (Colombia y Ecuador);
c) verificar la exactitud de sus declaraciones o entregar información, declaraciones o manifestaciones veraces, exactas y completas bajo su responsabilidad. (Ecuador y Perú);
d) actuar con diligencia para evitar el uso no autorizado de la Firma Electrónica.* (Ecuador y Venezuela); y
e) notificar que la Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada.* (Ecuador y Venezuela).

*Cabe destacar que las normas d) y e) han sido adoptadas en consonancia con disposiciones establecidas en la Ley Modelo de firmas electrónicas de la CNUDMI.

Si leemos detenidamente las disposiciones aquí transcritas, nos podremos percatar de que las legislaciones colombiana y peruana establecen las obligaciones del titular de una firma digital, mientras que las legislaciones ecuatoriana (proyecto de ley) y venezolana rigen las obligaciones del titular de una firma electrónica. Cabe mencionar, que las firmas digitales son una forma de firma electrónica y por lo tanto envuelven un concepto mas restringido que el de estas últimas.

El Decreto-Ley Venezolano estipula las obligaciones del signatario de la firma electrónica, mientras que los demás países rigen lo relacionado con el titular de la firma electrónica. Ecuador y Venezuela establecen las obligaciones del Titular o Signatario de la firma electrónica, mientras que Colombia y Perú rigen las obligaciones del Titular o Suscriptor de la firma digital. De esta manera, aparecen los tres conceptos utilizados como sinónimo indistintamente: titular, suscriptor y signatario.

Recomendación.
Si se pretenden armonizar las legislaciones en materia de comercio electrónico y afines de los países de la Comunidad Andina, recordamos que es imprescindible comenzar por una armonización de conceptos y definiciones para evitar confusiones futuras.

Venezuela adoptó una disposición semejante a la adoptada en Colombia, Ecuador y Perú sobre "mantener el control de la firma electrónica", al establecer que el signatario de la firma electrónica debe actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica, lo que implica, mantener el control de la misma.

No estaría de más agregar en una Decisión comunitaria, una regla similar a la contenida en la disposición venezolana que establece que en caso de incumplimiento de alguna de sus obligaciones, el signatario de la firma electrónica será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

"1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:
a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;
b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:
i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o
ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;
c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.
2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1."

C. Certificados Digitales:

1. ***Definición***

2. ***Requisitos para Obtener un Certificado Digital (Especificaciones Adicionales y Procedimiento)***

3. ***Contenido de un Certificado de Firma Electrónica***

4. ***Atribución Jurídica de un Certificado***

5. ***Duración del Certificado de una Firma Electrónica***

6. ***Aceptación de un Certificado, de un Mensaje de Datos o de una Firma Electrónica***

7. ***Obligaciones de los Suscriptores***

8. ***Suspensión, Revocación o Cancelación y Extinción de un Certificado***

   - ***8.1. Suspensión temporal del certificado digital***
   - ***8.2. Revocación del certificado digital***
   - ***8.3. Cancelación del certificado digital***
   - ***8.4. Extinción del certificado digital***

9. ***Certificaciones Recíprocas / Cruzadas***

C. Certificados Digitales:

Tal y como lo menciona Ysella Arguedas[35], "la firma digital no puede existir independientemente de un certificado digital que lo contenga, porque la firma, entendida como un conjunto de datos, es una característica del certificado".

Un certificado digital es un documento que permite identificar a la persona que usará la firma digital contenida en él, pues contiene los datos de su titular. El certificado digital contiene, igualmente, la clave pública del mismo, los datos y la firma digital de la Entidad / Autoridad de certificación que lo ha emitido.

Gracias al certificado digital, podemos confirmar que el firmante o signatario identificado en un certificado digital posee, de manera exclusiva, la clave privada correspondiente a la ya mencionada clave pública de dicho certificado.

Luego de esta breve introducción a los certificados digitales, pasaremos a analizar el contenido de las legislaciones sobre comercio electrónico de los países de la Comunidad Andina, y en particular, las disposiciones referentes a los certificados digitales.

[35] Analista Legal del Instituto Peruano de Comercio Electrónico -IPCE-.

C. Certificados Digitales:

1. Definición.

BOLIVIA – No posee actualmente legislación que regule los certificados digitales.

COLOMBIA – La Ley 527 define al certificado en relación con las firmas digitales como el mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste.

ECUADOR – La Ley ecuatoriana define el certificado de firma electrónica como el mensaje de datos que certifica la vinculación de una firma electrónica con una persona a través de un proceso de comprobación que confirma su identidad.

PERÚ – El Reglamento de la Ley 27.269 define al certificado digital como un documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

VENEZUELA - El Decreto-Ley venezolano define al certificado electrónico como el Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

Semejanzas y Diferencias. Comentarios.

Primeramente, podemos percatarnos de que se utilizaron diferentes nombres para definir los certificados digitales, pasando por certificados en relación con las firmas digitales hasta certificados electrónicos.

La definición colombiana menciona que el certificado contiene la clave pública del suscriptor, pero existen casos en los que el certificado contiene la clave privada del mismo, por lo que esta definición es muy limitativa y no elogia al principio de neutralidad tecnológica.

La definición peruana es la más cercana a las explicaciones aportadas por la antes citada Ysella Arguedas del Instituto Peruano de Comercio Electrónico y la misma posee todos los elementos integrantes de un certificado digital. Lo más importante es la mención a las claves (pública y privada) contenidas en el certificado que están vinculadas al titular del certificado, permitiendo su plena identificación; así como también, la indicación de que los certificados son emitidos y firmados digitalmente por una entidad de certificación y que los mismos constituyen un documento electrónico. La definición dada por la Ley ecuatoriana tiene características comunes con la peruana, pero la formulación de la disposición es diferente.

La definición venezolana no hace referencia al vínculo existente entre el par de claves y el titular del certificado ni sobre una de las potestades del certificado como lo es la posibilidad de identificar al titular del mismo gracias al uso de la tecnología criptográfica.

Recomendación.

Opinamos que “certificados digitales” es la palabra más corriente y conocida internacionalmente, por lo que aconsejamos se utilice éste término con preferencia a los demás (tal y como lo hizo Perú). En efecto, los demás términos pueden causar confusión.

C. Certificados Digitales:

2. Requisitos para Obtener un Certificado Digital (Especificaciones Adicionales y Procedimiento).

PERÚ - En el Reglamento de la Ley 27.269 se establecen los requisitos para obtener un certificado digital. Para la obtención de un certificado digital el solicitante deberá acreditar lo siguiente:

a. tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles; y
b. tratándose de personas jurídicas, acreditar la existencia de la misma y su vigencia mediante instrumentos públicos o norma legal respectivos.

Para ser titular de un certificado digital adicionalmente se deberá cumplir con: entregar la información solicitada por la entidad de certificación o la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.

En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular del certificado digital y de las firmas digitales que se generen.

Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado digital y de las firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Semejanzas y Diferencias. Comentarios.

Constatamos que únicamente el Perú se ha dado a la tarea de especificar los requisitos con los que deben cumplir personas naturales y jurídicas para solicitar y obtener un certificado digital. ¿No es ésta una facultad que debe ser atribuida a la Entidad / Autoridad de Certificación? Pensamos afirmativamente.

C. Certificados Digitales:

3. Contenido de un Certificado de Firma Electrónica.

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA – La Ley 527 pauta que un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

a. Nombre, dirección y domicilio del suscriptor.
b. Identificación del suscriptor nombrado en el certificado.
c. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
d. La clave pública del usuario.
e. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
f. El número de serie del certificado.
g. Fecha de emisión y expiración del certificado.

El Decreto 1747 indica que los certificados emitidos por las entidades de certificación cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor.

ECUADOR – El proyecto ecuatoriano considera que el certificado de firma electrónica para ser considerado válido deberá contener los siguientes requisitos:

a. identificación de la entidad de certificación de información.
b. domicilio legal de la entidad de certificación de información.
c. los datos del titular del certificado que permitan su ubicación e identificación.
d. el método de verificación de la firma del titular del certificado.
e. las fechas de emisión y expiración del certificado.
f. el número único de serie que identifica el certificado.
g. la firma electrónica de la entidad de certificación de información.
h. las limitaciones o restricciones para los usos del certificado; y
i. los demás señalados en esta Ley y los reglamentos.

PERÚ – La Ley 27.269 estipula que los certificados digitales emitidos por las entidades de certificación deben contener al menos:

a. Datos que identifiquen indubitablemente al suscriptor.
b. Datos que identifiquen a la Entidad de Certificación.
c. La clave pública.
d. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
e. Número de serie del certificado.
f. Vigencia del certificado.
g. Firma digital de la Entidad de Certificación.

El Reglamento de la Ley 27.269 prevé que los certificados digitales emitidos dentro de la Infraestructura Oficial de Firma Digital deberán contener como mínimo lo establecido en la Ley. La entidad de certificación podrá incluir, a pedido del solicitante del certificado digital, información adicional siempre y cuando la entidad de registro o verificación compruebe fehacientemente la veracidad de ésta.

VENEZUELA – El Decreto-Ley establece que los Certificados Electrónicos deberán contener la siguiente información:

a. identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica;
b. el código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica;
c. la identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica;
d. las fechas de inicio y vencimiento del período de vigencia del Certificado Electrónico;
e. la Firma Electrónica del Signatario;
f. un serial único de identificación del Certificado Electrónico; y

g. cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

Semejanzas y Diferencias. Comentarios.

Luego de una extensa investigación, llegamos a la conclusión de que los anteproyectos bolivianos no incluyen una disposición sobre contenido de los certificados digitales, por lo que trataremos, únicamente, el contenido de los ordenamientos jurídicos colombiano, ecuatoriano, peruano y venezolano.

De la lectura de la normativa aquí expuesta, nos hemos percatado de las semejanzas que existen en los Países Miembros de la Comunidad Andina en cuanto al contenido del certificado digital. Existe CONSENSO en lo que respecta a los siguientes requisitos:

a. nombre, dirección y domicilio del suscriptor o titular del certificado;
b. nombre, dirección y lugar donde realiza sus actividades la Entidad / Autoridad o Proveedor de servicios de certificación;
c. el serial único de identificación del Certificado Electrónico;
d. fecha de emisión y expiración del certificado;
e. la metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos (a excepción de Venezuela).

Estos requisitos deben figurar en todo certificado digital, tanto en Colombia, como en Ecuador, en Perú y en Venezuela.

Asimismo, tenemos disposiciones adoptadas por, no más de dos (02) países. Los requisitos en ellas contenidos son los siguientes:

a. La clave pública del usuario; (Colombia y Perú)
b. la firma electrónica* de la entidad de certificación de información (Ecuador y Perú)
c. Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico (Ecuador y Venezuela).

Éstos son requisitos exigidos en máximo dos (02) de los Países Miembros de la Comunidad.
*Perú se refiere a la firma digital, mientras que Ecuador se refiere a la firma electrónica. Como hemos venido expresando desde el inicio de la presente parte de este trabajo, estas disparidades deben ser subsanadas y un concepto único adoptado.

Consideramos que el requisito de código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica del texto venezolano podría equipararse con el requisito de la firma electrónica de la entidad de certificación de información que forma parte integrante de la normativa ecuatoriana y peruana.

Venezuela requiere, además, que la Firma Electrónica del Signatario figure en el certificado digital.

Recomendación.

Opinamos que un proyecto de Decisión para armonizar la legislación sobre comercio electrónico de los Países Miembros de la Comunidad debería incluir como principio general sobre el contenido de los certificados digitales, aquellos elementos que han sido unánimemente adoptados dentro del ordenamiento jurídico de los países involucrados.

C. Certificados Digitales:

4. Atribución Jurídica de un Certificado.

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - No posee disposiciones legales que traten este tema.

ECUADOR – El proyecto de Ley pauta que el certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento.

PERÚ - No posee disposiciones legales que traten este tema.

VENEZUELA – El Decreto-Ley estipula que el Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

Semejanzas y Diferencias. Comentarios.

Como pueden notar, Venezuela es el único país en haber adoptado una disposición legal que regule la atribución jurídica de un certificado digital. Tenemos nuestras dudas, respecto a la oportunidad de inserir una norma de este tipo en una Decisión comunitaria. En realidad esta norma es restrictiva y limitativa del alcance de la validez y efectos de un mensaje de datos o documento electrónico firmado digitalmente.

C. Certificados Digitales:

5. Duración del Certificado de una Firma Electrónica

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA – No posee disposiciones legales que traten este tema.

ECUADOR - Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a la Ley.

PERÚ – El Reglamento de la Ley estipula que el período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme a la Ley.

VENEZUELA – El Decreto-Ley establece que el Proveedor de Servicios de Certificación y el Signatario, de mutuo acuerdo, determinarán la vigencia del Certificado Electrónico. Igualmente, la ley establece dos causas expresas de cesación de la vigencia del certificado digital. Las causales son las siguientes:

a. cuando se produzca la extinción del signatario del certificado, o
b. cuando se produzca la incapacidad absoluta del signatario del certificado.

Semejanzas y Diferencias. Comentarios.

Hemos observado que Colombia no se pronunció sobre este tema. Observamos igualmente que la disposición venezolana, si bien es acertada, ya que por lo general, la vigencia del certificado es acordada de acuerdo al principio general de contratación reconocido internacionalmente [36]; la disposición peruana goza de mayor precisión.

Opinamos que la norma ecuatoriana remite a un reglamento actualmente inexistente para fijar el plazo de validez de los certificados de firma electrónica, creando así una inseguridad jurídica ... un vacío legal. Esperamos que la normativa relacionada con la duración del certificado en dicho reglamento a la Ley se acerque más al contenido de la normativa peruana.

Recomendación.

Consideramos que una Decisión comunitaria sobre comercio electrónico debería incluir una disposición sobre la duración de los certificados digitales y pensamos que el mejor modelo para ello, dentro de los textos legales de los Países Miembros de la Comunidad, es el peruano.

[36] Libertad de contratación.

C. Certificados Digitales:

6. Aceptación de un Certificado, de un Mensaje de Datos o de una Firma Electrónica.

COLOMBIA – La Ley 527 establece que, salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

Semejanzas y Diferencias. Recomendación.

Aunque ningún otro país de la subregión adoptare una disposición similar, consideramos que su contenido es plausible y podría ser objeto de incorporación en una Decisión comunitaria que armonice la legislación sobre comercio electrónico de los Países Miembros de la Comunidad.

C. Certificados Digitales:

7. Obligaciones de los Suscriptores.

PERÚ – Según el Reglamento de la Ley 27.269, son obligaciones del titular de certificado digital:

a. Actualizar permanentemente la información proveída tanto a la entidad de certificación como a la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.
b. Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
c. Observar permanentemente las condiciones establecidas por la entidad de certificación para la utilización del certificado digital.

Semejanzas y Diferencias. Comentarios.

Primeramente, observamos que la normativa colombiana, ecuatoriana y venezolana se refieren únicamente a los deberes y / u obligaciones del suscriptor o titular de la firma electrónica, mientras que Perú regula tanto esto último como las obligaciones del titular del certificado digital.
Consideramos que a los efectos de una armonización de la normativa legal sobre comercio electrónico, debe llegarse a un consenso en el que se decida regular:

- los deberes y obligaciones del titular o suscriptor de la firma digital (que está, obviamente, contenida en un certificado digital), o
- los deberes y obligaciones del poseedor o suscriptor de un certificado digital, o
- ambas disposiciones.

Pasemos ahora a analizar el texto:
Perú establece que el Suscriptor o Titular del certificado debe solicitar la revocación o cancelación de su certificado ante la Entidad de Certificación. En el caso colombiano, cuando se hace referencia a los deberes del suscriptor de la firma digital, se establece que esta solicitud debe hacerse "oportunamente"; mientras que en el caso del Perú, la solicitud debe hacerse en un caso concreto, es decir, cuando la reserva sobre la clave privada se haya visto comprometida. Aconsejamos ser explícitos en cuanto a los motivos por los cuales el suscriptor o titular del certificado debe solicitar la revocación o cancelación de su certificado.

Recomendación.

Las disposiciones de la legislación peruana en materia de obligaciones del titular de certificado digital, sobre actualizar permanentemente la información proveída tanto a la entidad de certificación como a la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta y observar permanentemente las condiciones establecidas por la entidad de certificación para la utilización del certificado digital, son loables y podrían ser consideradas como base para los lineamientos de una futura armonización de normas sobre comercio electrónico en el seno de la Secretaría de la Comunidad Andina.

C. Certificados Digitales:

8. Suspensión, Revocación o Cancelación y Extinción de un Certificado.

8.1. Suspensión temporal del certificado digital:

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - No posee disposiciones legales que traten este tema.

ECUADOR – De conformidad con el proyecto ecuatoriano, la entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a. sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley;
b. se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y
c. se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.
La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

PERÚ - No posee disposiciones legales que traten este tema. De acuerdo con la normativa peruana, los certificados pueden, únicamente, ser cancelados por determinadas causales, entre ellas, la cancelación por revocación.

VENEZUELA - Suspensión temporal voluntaria. El Signatario podrá solicitar la suspensión temporal del Certificado Electrónico, de conformidad con el Decreto-Ley, en cuyo caso su Proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el Signatario.

Suspensión o revocatoria forzosa. Decreto-Ley. En los contratos que celebren los Proveedores de Servicios de Certificación con sus usuarios, se deberán establecer como causales de suspensión o revocatoria del Certificado Electrónico de la Firma Electrónica, las siguientes:

a. Sea solicitado por una autoridad competente de conformidad con la ley.
b. Se compruebe que alguno de los datos del Certificado Electrónico proporcionado por el Proveedor de Servicios de Certificación es falso.
c. Se compruebe el incumplimiento de una obligación principal derivada del contrato celebrado entre el Proveedor de Servicios de Certificación y el Signatario.
d. Se produzca una Quiebra Técnica del sistema de seguridad del Proveedor de Servicios de Certificación que afecte la integridad y confiabilidad del certificado contentivo de la Firma Electrónica.

Asimismo, se preverá en los referidos contratos que los Proveedores de Servicios de Certificación podrán dejar sin efecto la suspensión temporal del Certificado Electrónico de una Firma Electrónica al verificar que han cesado las causas que originaron dicha suspensión, en cuyo caso el Proveedor

de Servicios de Certificación correspondiente estará en la obligación de habilitar de inmediato el Certificado Electrónico de que se trate.

La vigencia del Certificado Electrónico cesará cuando se produzca la extinción o incapacidad absoluta del Signatario.

8.2. Revocación del certificado digital:

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo, de conformidad con la Ley 527. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

a. Por pérdida de la clave privada.
b. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.
Una entidad de certificación revocará un certificado emitido por las siguientes razones:

a. A petición del suscriptor o un tercero en su nombre y representación.
b. Por muerte del suscriptor.
c. Por liquidación del suscriptor en el caso de las personas jurídicas.
d. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
e. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
f. Por el cese de actividades de la entidad de certificación, y
g. Por orden judicial o de entidad administrativa competente.

Según el Decreto 1747, cada certificado revocado debe indicar si el motivo de revocación incluye la pérdida de control de la clave privada, evento en el cual, las firmas generadas con dicha clave privada carecerán del atributo de unicidad previsto en el numeral 1 del parágrafo del artículo 28 de la Ley 527 de 1999, salvo que se demuestre lo contrario, mediante un mecanismo adicional que pruebe inequívocamente que el documento fue firmado digitalmente en una fecha previa a la revocación del certificado.

Las revocaciones deberán ser publicadas de manera inmediata en los repositorios correspondientes y notificadas al suscriptor dentro de las 24 horas siguientes. Si dichos repositorios no existen al momento de la publicación del aviso, ésta se efectuará en un repositorio que designe la Superintendencia de Industria y Comercio.

ECUADOR - El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando:

a. La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y
b. Se produzca la quiebra técnica de la entidad de certificación.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

PERÚ - La Entidad de Certificación revocará el certificado digital en los siguientes casos establecidos en la Ley 27.269:

a. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
b. Por muerte del titular de la firma digital.
c. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

De acuerdo con el Reglamento de Ley 27.269, para efectos de la cancelación de oficio o revocación de certificados digitales, la entidad de certificación debe contar con procedimientos detallados en su declaración de prácticas de certificación.

La revocación también puede ser solicitada por un tercero que informe fehacientemente de alguno de los supuestos de revocación de la Ley.

La revocación debe indicar el momento desde el cual se aplica, precisando como mínimo la fecha y el tiempo del mismo, que deberá estar expresado en minutos y segundos.

La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La entidad de certificación debe inmediatamente incluir la revocación del certificado en la relación que corresponda.

VENEZUELA - Revocatoria forzosa pautada por el Decreto-Ley. En los contratos que celebren los Proveedores de Servicios de Certificación con sus usuarios, se deberán establecer como causales de suspensión o revocatoria del Certificado Electrónico de la Firma Electrónica, las siguientes:

a. Sea solicitado por una autoridad competente de conformidad con la ley.
b. Se compruebe que alguno de los datos del Certificado Electrónico proporcionado por el Proveedor de Servicios de Certificación es falso.
c. Se compruebe el incumplimiento de una obligación principal derivada del contrato celebrado entre el Proveedor de Servicios de Certificación y el Signatario.
d. Se produzca una Quiebra Técnica del sistema de seguridad del Proveedor de Servicios de Certificación que afecte la integridad y confiabilidad del certificado contentivo de la Firma Electrónica.

8.3. Cancelación del certificado digital.

BOLIVIA – No posee disposiciones legales que traten este tema.

COLOMBIA - No posee disposiciones legales que traten este tema.

ECUADOR - No posee disposiciones legales que traten este tema.

PERÚ – Según la Ley 27.269 y el Reglamento de la Ley, la cancelación del certificado digital puede darse:

a. Por solicitud del titular de la firma digital.
b. Por revocatoria de la entidad de certificación, con expresión de la causa.
c. Por expiración del plazo de vigencia.
d. Por solicitud del titular sin previa justificación, siendo necesaria para tal efecto la aceptación y autorización de la entidad de certificación o la entidad de registro o verificación, según sea el caso. La misma que deberá ser aceptada y autorizada como máximo dentro del plazo establecido por la autoridad administrativa competente, si en el plazo indicado la entidad no se pronuncia, se entenderá la cancelación del certificado; la misma que no podrá ser opuesta al tercero de buena fé.
e. Por el cese de operaciones de la entidad de certificación que lo emitió.
f. Por resolución administrativa o judicial que lo ordene.
g. Por interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta, del titular del certificado digital.
h. Por extinción de la personería jurídica o declaración judicial de quiebra.
i. Otras causales que establezca la autoridad administrativa competente.

La solicitud de cancelación de un certificado digital puede ser realizada por su titular o a través de un representante debidamente acreditado; pudiendo realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las entidades de certificación.

El titular del certificado digital está obligado a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:
a. Por exposición, puesta en peligro o uso indebido de la clave privada.
b. Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
Si en estos casos el titular no solicita la cancelación, será responsable por los daños o perjuicios generados a terceros de buena fe que confiaron en el contenido del certificado.

VENEZUELA - La cancelación de un Certificado Electrónico procederá, según lo estipulado en el Decreto-Ley, cuando el Signatario así lo solicite a su Proveedor de Servicios de Certificación. Dicha cancelación no exime al Signatario de las obligaciones contraídas durante la vigencia del Certificado, conforme a lo previsto en este Decreto-Ley.

El Signatario estará obligado a solicitar la cancelación del Certificado Electrónico cuando tenga conocimiento del uso indebido de su Firma Electrónica. Si el Signatario en conocimiento de tal situación no solicita dicha cancelación, será responsable por los daños y perjuicios sufridos por terceros de buena fe como consecuencia del uso indebido de la Firma Electrónica certificada mediante el correspondiente Certificado Electrónico.

8.4. Extinción del certificado digital

ECUADOR - Los certificados de firma electrónica, se extinguen, por las siguientes causas:
a. solicitud de su titular;
b. extinción de la firma electrónica; y
c. expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Semejanzas y Diferencias. Comentarios.

Como punto de partida, podemos observar que la suspensión temporal del certificado digital ha sido prevista en Ecuador y Venezuela. Las legislaciones colombiana y peruana no prevén esta figura.

En segundo lugar, podemos observar que los certificados digitales pueden ser revocados de conformidad con la legislación existente en Colombia, Ecuador, Perú y Venezuela.

A su vez, Perú y Venezuela han establecido en sus legislaciones respectivas, la llamada cancelación del certificado digital, mientras que la normativa ecuatoriana se refiere a la extinción del certificado digital. Cabe destacar que, la norma jurídica colombiana no hace mención a las figuras de “cancelación” ni “extinción” del certificado digital.

Pasemos ahora a analizar las causales de suspensión temporal, revocación, cancelación y / o extinción del certificado digital:

- Las ***causales de suspensión temporal*** de las legislaciones ecuatoriana y venezolana son muy similares. A pesar de ello, la normativa venezolana ha previsto dos tipos de suspensión temporal del certificado digital: la voluntaria, cabe decir, la solicitada por el signatario o titular del certificado, y la forzosa. Ecuador solo prevé la suspensión temporal forzosa del certificado digital.

  Tres son las causales principales de suspensión temporal “forzosa” del certificado, de conformidad con las mencionadas normativas legales:
  a. en caso de ser dispuesto por la autoridad competente, que en el caso del Ecuador es el Consejo Nacional de Telecomunicaciones (CONATEL),

b. en caso de que la entidad de certificación de información o proveedor de servicios de certificación compruebe falsedad de alguno de los datos consignados por el titular del certificado y contenidos en este último y,
c. en caso de que se produzca el incumplimiento de alguna de las obligaciones contractuales contraídas entre la entidad de certificación de información o proveedor de servicios de certificación y el titular o signatario del certificado digital. Cabe mencionar, que la disposición ecuatoriana dispone "en caso de que se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información "y el titular de la firma digital". Creemos que la redacción debería decir "y el titular del certificado digital". Es decir, creemos que colocar "el titular del certificado digital" es más pertinente en este caso, en vista de que estamos refiriéndonos a las causales de suspensión de certificados digitales que generan o contienen la firma digital.

Las disposiciones legales venezolanas establecen una cuarta (4ta.) causal de suspensión temporal del certificado digital, en caso de que se produzca una quiebra técnica del sistema de seguridad del proveedor de servicios de certificación afectando así la integridad y confiabilidad del certificado contentivo de la firma electrónica. La Ley Ecuatoriana ha previsto esta situación como causal de REVOCACIÓN del certificado digital.

Ambos países estipulan que cuando cesen las causas objeto de la suspensión temporal de un certificado digital, el mismo deberá ser habilitado inmediatamente por la entidad o proveedor de servicios de certificación que lo emitió, dejando de esta manera, sin efecto la suspensión temporal. El Ecuador incluyó, además, un segundo motivo por el cual debe habilitarse nuevamente un certificado digital que haya sido suspendido. Esta situación se presenta cuando mediare una resolución del CONATEL.

La Ley Ecuatoriana regula, de igual manera, la notificación de la suspensión del certificado y el momento en el cual surte efecto la suspensión temporal. A su vez, la misma establece que la responsabilidad por los posibles daños y perjuicios que puedan ocasionarse por falta de comunicación o publicación o retraso en la publicación de la suspensión temporal recaerá sobre la entidad de certificación de información.

El artículo ecuatoriano dispone, igualmente, que el titular del certificado de la firma electrónica NO QUEDA EXIMIDO de las obligaciones que haya contraído previamente a la suspensión de su certificado y que hayan sido derivadas del uso del mismo.

- Seguidamente, presentaremos las semejanzas y diferencias de las legislaciones de los países de la Comunidad Andina en materia de ***revocación de certificados digitales***.

Dentro de tantas posiciones y diferencias, podemos identificar las causales de revocación de certificados digitales que se repiten en, al menos, dos de las legislaciones bajo estudio:
a. Por muerte del titular o suscriptor de la firma digital (Colombia y Perú).
b. Por el cese de actividades de la entidad de certificación (Colombia y Ecuador*). La Ley Ecuatoriana agrega, que habrá revocatoria de los certificados en caso de cesación de las actividades de la entidad de certificación, si y sólo si, aquellos no son asumidos por otra entidad de certificación.
c. Por una Quiebra Técnica del sistema de seguridad de la Entidad o Proveedor de Servicios de Certificación (Ecuador* y Venezuela). El segundo de los países mencionados, prevé esta situación, tanto como causal de suspensión forzosa como causal de revocación del certificado digital. Además, agrega que la quiebra técnica debe afectar la integridad y confiabilidad del certificado contentivo de la Firma Electrónica.
d. Por el incumplimiento de las obligaciones contractuales contraídas entre la Entidad o Proveedor de Servicios de Certificación y el Signatario (Perú y Venezuela). El Decreto-Ley venezolano, dispone además, que se procederá a la revocatoria del certificado solo en caso de incumplimiento de una obligación principal derivada del contrato.
e. Porque se compruebe o determine que alguno de los datos del Certificado Electrónico o Digital es falso, inexacto o ha sido modificado (Colombia, Perú y Venezuela). Cabe destacar, que la disposición venezolana se refiere a los certificados, como certificados electrónicos, y no digitales, como aparece mencionado en las legislaciones de los demás países de la Comunidad Andina.

* La gran diferencia que existe entre la normativa ecuatoriana y el resto de las legislaciones, es que el órgano regulador de las entidades de certificación, es decir CONATEL, es quien está facultado para revocar certificados digitales de firma electrónica por las dos causales señaladas *supra*. El Decreto-Ley Venezolano, establece que la revocatoria de un certificado electrónico puede ser solicitada por una autoridad competente. Creemos que esa autoridad competente es el órgano regulador de las entidades de certificación, en este caso, la Superintendencia de Certificación. La Legislación peruana solo menciona que la revocación puede ser solicitada por un tercero haciendo valer la existencia de alguna de las causales mencionadas precedentemente.

La normativa colombiana establece que el suscriptor de una firma digital certificada o su representante, podrán solicitar la revocación del certificado por pérdida de la clave privada o, en caso de que esta última, haya sido expuesta o corra peligro de que sea usada indebidamente. Si el suscriptor no cumple con su deber de solicitar la revocación, será responsable por las pérdidas o perjuicios incurridos por terceros de buena fe.

Colombia, Ecuador y Perú regulan lo referente a la notificación y publicación de la revocación de los certificados digitales, mientras que Venezuela nada dice al respecto. La ley de Comercio Electrónico del Ecuador prevé a partir de qué momento surte efectos la revocación del certificado frente a terceros y a su titular. De conformidad con esta novedosa Ley, la entidad de certificación es responsable por la no-comunicación y publicación (o retraso) de la revocación.

La Ley venezolana, establece que el contrato entre la entidad o proveedor de servicios de certificación y el usuario del certificado debe estipular las causales de revocación del certificado electrónico. Por su parte, la legislación peruana establece que la entidad de certificación debe estipular un procedimiento detallado en su declaración de prácticas de certificación.

La reciente Ley ecuatoriana, es la única a estipular que la revocatoria del certificado no exime al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso. Y el Perú es el único que posee una normativa que establece que la revocación de un certificado no puede ser aplicada retroactivamente.

Recomendación.

Realmente nos preocupa la disparidad existente en materia de causales de revocación de certificados digitales existente actualmente en las legislaciones de los Países Miembro de la Comunidad Andina. Recomendamos la búsqueda de un consenso en materia de causales de revocación de certificados digitales.

- La ***cancelación de certificados digitales*** ha sido prevista por Perú y Venezuela. Ambos acuerdan en cancelar un certificado previa solicitud del titular o signatario de la firma digital.

  Ambos países establecen que es deber del titular o signatario del certificado solicitar la cancelación del certificado en caso de que la clave privada haya sido expuesta o puesta en peligro o esté siendo usada indebidamente. Las disposiciones peruana y venezolana regulan además, que si el titular no cumple con su deber de solicitar la cancelación del certificado cuando tenga conocimiento del uso indebido de su firma, el mismo será responsable por las pérdidas o perjuicios incurridos por terceros de buena fe como consecuencia del uso indebido del certificado.

  La norma peruana también estipula que el titular del certificado debe solicitar su cancelación por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada. También autoriza la solicitud de cancelación del certificado por parte de su titular, sin previa justificación.

  Recordemos que las disposiciones colombianas prevén que estas causales relacionadas con la clave privada del certificado ocasionan la revocación del certificado.

  Establece la ley venezolana, que la cancelación del certificado no exime al signatario del certificado de firma electrónica, de las obligaciones derivadas de su uso contraídas durante la vigencia del mismo.

La normativa peruana, igualmente, faculta al representante del titular de un certificado a solicitar la cancelación de este último.

El Proyecto de Ley peruano establece como causales de cancelación del certificado, circunstancias que han sido consideradas por la legislación Colombiana, por dar un ejemplo, como causales de revocación del certificado. Estas causales son las siguientes:

a. El cese de operaciones de la entidad de certificación que lo emitió.
b. La resolución judicial que lo ordene.
c. En caso de muerte, interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta.

La expiración del plazo de vigencia, establecido como causal de cancelación del certificado de acuerdo a la normativa peruana, ha sido establecido como causal de extinción del certificado por la Ley ecuatoriana.

Para concluir, cabe mencionar que la revocatoria del certificado realizada por la entidad de certificación es una causal de cancelación del certificado, de conformidad con lo dispuesto en la legislación peruana.

- El comentario principal que podemos emitir al referirnos a la ***extinción de certificados digitales***, es que el único país en haber adoptado esta figura es Ecuador. La legislación ecuatoriana prevé tres causales de extinción del certificado digital de firma electrónica. La primera tiene lugar a solicitud del titular de la firma; la segunda ocurre por extinción de la firma electrónica y la tercera, por expiración del plazo de validez del certificado (esta última es una causal de cancelación del certificado para el Perú).

  La Ley de Comercio Electrónico del Ecuador prevé a partir de qué momento surte efectos la revocación del certificado frente a terceros y a su titular. Asimismo establece que la extinción del certificado no exime al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

Recomendación.

Consideramos pertinente recomendar, que en una futura Decisión comunitaria para la armonización de la legislación de comercio electrónico de los Países Miembro de la Comunidad Andina, se establezcan únicamente las figuras de la suspensión y de la revocación de los certificados digitales de firma electrónica. Ello con el ánimo de evitar confusiones entre lo que se entienda por cancelación, revocación y extinción del certificado digital y sus respectivos efectos legales. En vista de que las causales de cancelación, revocación y extinción son, en su mayoría las mismas, no debe ser difícil llegar a una aceptación unánime de la figura de la revocación que se adopte en reemplazo de las figuras de cancelación y extinción de certificados.

C. Certificados Digitales:

9. *Certificaciones Recíprocas / Cruzadas[37].*

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA – De acuerdo a la Ley 527, los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Los certificados recíprocos deben contener[38] al menos la siguiente información:

a. Identificador único del certificado.
b. Clave pública de la entidad que se está reconociendo.
c. Tipos de certificados a los que se remite el reconocimiento.
d. Duración del reconocimiento.
e. Referencia de los límites de responsabilidad del tipo de certificado al cual se remite el reconocimiento.

Según el Decreto 1747, el reconocimiento de los certificados de firmas digitales emitidos por entidades de certificación extranjeras, realizado por entidades de certificación autorizadas para tal efecto en Colombia, se hará constar en un certificado expedido por estas últimas. El efecto del reconocimiento de cada certificado, se limitará a las características propias del tipo de certificado reconocido y por el período de validez del mismo.
Los suscriptores de los certificados reconocidos y los terceros tendrán idénticos derechos que los suscriptores y terceros respecto de los certificados propios de la entidad que hace el reconocimiento.

ECUADOR – El proyecto de Ley establece que los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador[39]**.** (Esta disposición es similar a la estipulada en la Ley Modelo sobre firmas electrónicas de la CNUDMI[40])

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta Ley y su reglamento.

---

[37] Certificación cruzada: es el acto por el cual una entidad de certificación acreditada reconoce la corrección y validez de un certificado digital emitido por otra entidad de certificación, sea nacional, extranjera o internacional, previa autorización de la autoridad administrativa competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad. (Reglamento Ley 27.269 peruana)

[38] El contenido de los certificados recíprocos es determinado por el órgano de regulación y control de las entidades / autoridades de certificación, en este caso, por la Superintendencia de Industria y Comercio.

[39] El órgano de regulación de las entidades / autoridades de certificación, en este caso, El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de esta disposición.

[40] Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras en la Ley Modelo de firmas electrónicas de la CNUDMI: "1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.

2. Todo certificado expedido fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

3. Toda firma electrónica creada o utilizada fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que toda firma electrónica creada o utilizada en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2., o del párrafo 3., se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2., 3. y 4., las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable."

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho. (Esta disposición es similar a la estipulada en la Ley Modelo sobre firmas electrónicas de la CNUDMI.)

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

Los certificados de firmas electrónicas, emitidos por entidades de certificación extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la Ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

PERÚ – La Ley 27.269 prevé que los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente.

La autoridad administrativa competente podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de certificados digitales otorgados en el extranjero y extender la validez de la Infraestructura Oficial de Firma Digital. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley como en el Reglamento; de conformidad con lo pautado en el Reglamento de Ley 27.269.

La autoridad administrativa competente podrá reconocer certificados digitales emitidos por entidades extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las mismas que deben velar por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento y u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas entidades de certificación nacionales que utilicen servicios de entidades de certificación extranjeras, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para los efectos de lo dispuesto en el párrafo precedente, la entidad extranjera deberá comunicar a la autoridad administrativa competente el nombre de aquellas entidades que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.

La autoridad administrativa competente emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así como los mecanismos adecuados de información a los agentes del mercado.

Las entidades de certificación acreditadas pueden realizar certificaciones cruzadas con entidades de certificación extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero incorporándolos como suyos dentro de la Infraestructura Oficial de Firma Digital de conformidad con la Ley, siempre y cuando obtengan autorización previa de la autoridad administrativa competente.

Las entidades de certificación acreditadas que realicen certificaciones cruzadas, garantizarán ante la autoridad administrativa competente que los certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la Infraestructura Oficial de Firma Digital, y que cumplen las funciones señaladas en la Ley.

Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.

Las entidades de certificación acreditadas que realicen certificaciones cruzadas conforme al primer párrafo del presente artículo, garantizarán ante la autoridad administrativa competente que los certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la

Infraestructura Oficial de Firma Digital, y que cumplen las funciones señaladas en el artículo 2º de la Ley.

VENEZUELA – De conformidad con el Decreto-Ley, bs Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado.

Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

Semejanzas y Diferencias. Comentarios.

Luego de una lectura detallada del contenido de las diferentes disposiciones sobre certificación cruzada y recíproca, hemos llegado a la conclusión de que hay un PRINCIPIO GENERAL en el que se basan las disposiciones del Ecuador, de Perú y de Venezuela. Este principio es el siguiente: los Certificados Electrónicos emitidos por entidades / autoridades o proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica que los certificados digitales emitidos en el territorio nacional de cada país.

Cabe destacar que la redacción en el Ecuador difiere un poco de la Peruana y la Venezolana, pues la misma establece, únicamente, que los certificados digitales emitidos en el extranjero tienen el mismo valor legal en Ecuador que los certificados emitidos en ese país. A pesar de ello, encontramos mucha semejanza entre las frases “mismo valor legal” y “misma validez y eficacia jurídica”, por lo que hemos considerado que los tres países mencionados en el párrafo anterior, han regulado la certificación cruzada / recíproca partiendo de una misma y uniforme base legal.

Por el contrario, Colombia fue el único país en haber adoptado como principio general, el siguiente: los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos. Cabe notar, que la disposición no se refiere en ningún momento al tipo de validez y eficacia jurídica o valor jurídico que se le atribuyen en ese país a los certificados digitales emitidos en el extranjero.

Habiendo identificado el principio general en el que se basó el Legislador, pasaremos a identificar las condiciones necesarias para que la regla se cumpla.

En Colombia, Ecuador, Perú y Venezuela, para ser reconocidos como válidos y surtan plenos efectos jurídicos, los certificados digitales emitidos en el extranjero que se deseen reconocer en el país en cuestión, deben cumplir con los mismos requisitos legales establecidos para la emisión de certificados por parte de las entidades de certificación nacionales y / o la autoridad administrativa o entidad / autoridad / o proveedor de servicios de certificación autorizada(o) para ello.

Adicionalmente, quien reconozca validez y eficacia jurídica a tales certificados digitales emitidos en el extranjero, deberá garantizar el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado en la misma forma que lo hace con sus propios certificados.

En Ecuador, los certificados digitales emitidos en el extranjero reconocidos en el país, deben, además, presentar un grado de fiabilidad equivalente al de los certificados digitales emitidos en el país por la entidad de certificación de información acreditada. El grado de fiabilidad, es un tema que ha sido desarrollado por la CNUDMI en su Ley Modelo de firmas electrónicas. Les recomendamos la lectura de la Ley Modelo, para obtener una mejor comprensión y alcance de esta disposición.

Aclarado esto, pasemos a identificar qué órgano está facultado para reconocer, en el país que corresponda, certificados digitales emitidos en el extranjero:

- En Colombia, es la Entidad de Certificación abierta (autorizada para ello por el órgano regulador, que en este caso es la Superintendencia de Industria y Comercio) quien podrá reconocer certificados digitales emitidos en el extranjero.
- En el Ecuador, solo la entidad de certificación de información acreditada (por el Consejo Nacional de Telecomunicaciones [CONATEL], órgano regulador) podrá reconocer certificados digitales emitidos en el extranjero.
- En Perú, la autoridad administrativa competente, Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual (INDECOPI) en este caso, o la Entidad de Certificación acreditada (autorizada para ello por la autoridad administrativa), pueden reconocer certificados digitales emitidos en el extranjero.
- En Venezuela, los certificados deben ser reconocidos por un proveedor de servicios de certificación acreditado (por la Superintendencia de Servicios de Certificación Electrónica, órgano regulador y de control[41]).

Recomendación.

RECONOCIMIENTO DE CERTIFICADOS DIGITALES EMITIDOS FUERA DE LA COMUNIDAD ANDINA (CERTIFICADOS DIGITALES EXTRA-COMUNITARIOS): A los fines de una armonización de las diferentes normas legales, recomendamos que todos los países acuerden que una Entidad / Autoridad / Proveedor de Servicios de Certificación legalmente constituida, podrá reconocer certificados digitales emitidos fuera del territorio de la Comunidad Andina, sin necesidad de solicitar autorización previa por parte del órgano regulador de dichas Entidades.

Asimismo, y con ánimo de establecer garantías, consideramos que una Decisión comunitaria sobre este tema debe incluir además, la siguiente regla: Los certificados digitales emitidos en el extranjero, reconocidos por una Entidad de Certificación, deben cumplir con los mismos requisitos legales establecidos para la emisión de certificados digitales nacionales. En consecuencia, la entidad que reconozca tales certificados digitales emitidos en el extranjero, deberá garantizar el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado en la misma forma que lo hace con sus propios certificados.

RECONOCIMIENTO DE CERTIFICADOS DIGITALES EMITIDOS DENTRO DE LA COMUNIDAD ANDINA (CERTIFICADOS DIGITALES COMUNITARIOS): Opinamos que, con el objetivo de eliminar los obstáculos al reconocimiento de certificados digitales emitidos por entidades de certificación de origen Andino, es decir, con sede en alguno de los cinco (5) Países Miembros de la Comunidad Andina, debe establecerse como regla general que, serán reconocidos, dentro del territorio de la Comunidad, todos aquellos certificados digitales que cumplan con los requisitos de seguridad, de validez y de vigencia de los certificados digitales establecidos en "X" Decisión comunitaria.

Es necesario evitar la inclusión de procedimientos engorrosos como los que exigen autorización por parte de un órgano de regulación o autoridad administrativa cada vez que se vaya a reconocer un certificado. Si el órgano regulador de las entidades de certificación desea llevar un registro de los certificados reconocidos, basta con incluir en la debida Decisión comunitaria, en la parte relacionada con las obligaciones de las entidades de certificación, EL DEBER DE LAS ENTIDADES DE CERTIFICACIÓN DE NOTIFICAR AL ÓRGANO REGULADOR EL (O LOS) CERTIFICADO(S) DIGITAL(ES) COMUNITARIO(S) Y / O EXTRA-COMUNITARIO(S) (DATOS DEL CERTIFICADO) QUE HAYA(N) SIDO RECONOCIDO(S).

Antes de pasar al siguiente tema, sugerimos el establecimiento de la presunción *iuris tantum* (salvo prueba en contrario) de la validez y eficacia a todos los certificados digitales, independientemente de la tecnología, emitidos por entidades de certificación (cerrada; no acreditada; no autorizada), siempre y cuando se cumplan con ciertos requisitos. Los requisitos básicos deberían ser adoptados por todos los países, gracias a una Decisión comunitaria y la aplicación de los mismos deberían depender de las resoluciones de las autoridades administrativas competentes (órganos reguladores). Ello no es un inconveniente, siempre y cuando, se sienten las bases de dichos requisitos en una norma supranacional que tome en consideración el principio de neutralidad tecnológica estudiado en capítulos precedentes.

[41] Ésta Superintendencia tiene por objeto acreditar y controlar a los proveedores de servicios de certificación públicos o privados. (Ver artículo 20 de la Ley sobre mensajes de datos y firmas electrónicas de Venezuela [Decreto 1.024])

D. Entidades / Autoridades de Certificación y Registro:

1. ***Definición, características y requerimientos de las entidades de certificación***

2. ***Entidades de Registro***

D. Entidades / Autoridades de Certificación y Registro:

Según las palabras del Sr. Oliver Muñoz Esquivel, Abogado panameño especializado en Derecho Mercantil Internacional en los Estados Unidos de América, "...Las entidades de certificación tienen como fin primordial garantizar el principio de equivalencia funcional de los mensajes electrónicos de datos *vis a vis* de los documentos tradicionales o en papel. Para tales fines, las entidades de certificación efectúan un proceso de validación o autenticación de la identidad de los emisores y receptores que envían o reciben los mensajes firmados digitalmente...como parte de sus funciones, las entidades de certificación mantienen un registro y estampado cronológico en la transmisión y recepción de los mensajes de datos, lo que permite verificar que un mensaje de datos ha sido efectivamente enviado por su emisor y recibido por su destinatario.", entre otras cosas.

EL Sr. Muñoz sostiene que existen varias teorías o posturas sobre la figura de la entidad de certificación. Nosotros reproduciremos en este trabajo lo relativo a lo que el escritor ha calificado como la teoría o postura privatista. Esta postura sostiene que la actividad de las entidades de certificación es de carácter privado y que la misma puede estar sujeta a las reglas del mercado.

En consecuencia, "la actividad de las entidades de certificación no ha de estar sujeta a autorización previa por parte del Estado...la misma debe regirse por las reglas del mercado, esto es, con base a un régimen de libre competencia..."

La Prof. Maria de los Ángeles Martín Reyes de la Universidad de Málaga - España, nos comenta que, el Parlamento Europeo fundamenta la ausencia de controles administrativos previos y de exigibilidad de unos requisitos mínimos a acreditar para ejercer las funciones de certificación, argumentando que la ausencia de control previo facilita, a la entidad que desee ejercer tales funciones, el acceso a la condición de prestador de servicios de certificación.

Y en consonancia con la postura o teoría privatista mencionada por el Ab. Muñoz, la Prof. Martín considera que el libre acceso al ejercicio de las funciones de certificación y la libre competencia, determinará que sea el propio mercado el que proceda a eliminar a los prestadores de servicios de certificación que no obren de conformidad a las exigencias de aquel.

Es de importancia capital, acoger en futuras legislaciones o en una Decisión comunitaria, el principio de la libre competencia con respecto a las entidades de certificación y registro, tal como lo hace el Reglamento peruano al establecer que LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ASÍ COMO LOS DE REGISTRO O VERIFICACIÓN SE REALIZA EN EL **RÉGIMEN DE LIBRE COMPETENCIA**.

Luego de esta breve introducción, pasemos al análisis de las disposiciones previstas en los Países Miembros de la Comunidad Andina sobre entidades de certificación. Los siguientes temas no serán tratados en la presente versión de este reporte: Actividades y Funciones de las Entidades de Certificación; Deberes y Responsabilidades de las Entidades de Certificación; Término de Conservación de los Registros; Remuneración de las Entidades de Certificación por la Prestación de Servicios; Cese de las Actividades de la Entidad de Certificación; Terminación Unilateral / Terminación Contractual; Auditoría de las entidades; los Órganos de Control, de Acreditación y de Regulación de Registro o Verificación y Régimen de Acreditación de las Mismas; Infracciones, Sanciones y Medidas Preventivas y Cautelares y la Cancelación de la Acreditación.

D. Entidades / Autoridades de Certificación y Registro:

1. Definición, características y requerimientos de las entidades de certificación.

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - Según la Ley 527, podrán ser entidades de certificación[42], las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

a. Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.
b. Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.
c. Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

Autorización de entidad de certificación cerrada, de conformidad con la Resolución 26.930. La persona que solicite autorización como entidad de certificación cerrada, según lo dispuesto en el decreto 1747 de 2000, deberá demostrar el cumplimiento de las condiciones establecidas en la ley 527 de 1999 y el decreto 1747, para lo cual deberá diligenciar el Anexo 1 de la Resolución y adjuntando la siguiente información:

a. Certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.
b. Un formato diligenciado del Anexo 2 por cada uno de los administradores o representantes legales.

Cambio de servicios ofrecidos en entidad de certificación cerrada, de acuerdo a lo pautado en la Resolución 26.930. Cuando la entidad de certificación cerrada pretenda ofrecer nuevos servicios como entidad de certificación dentro del entorno cerrado, según lo dispuesto en el Decreto 1747, deberá solicitar autorización previa ante esta Superintendencia, mediante el diligenciamiento del Anexo 4.

Autorización de entidad de certificación abierta, según lo dispone la Resolución 26.930. La persona que solicite autorización como entidad de certificación abierta según lo dispuesto en el decreto 1747, deberá demostrar que la actividad está prevista en el objeto social principal, el cumplimiento de las condiciones establecidas en la Ley 527 y el Decreto 1747 y los estándares, planes y procedimientos de seguridad establecidos en la sección V de esta resolución, diligenciando el Anexo 1 y adjuntando la siguiente información:

a. Anexo 2 debidamente diligenciado por cada uno de los administradores o representantes legales adjuntando:
b. Certificado judicial vigente o documento equivalente proveniente del país o países donde haya residido.
c. Copia del certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.
d. Copia del acto que le otorga la personería jurídica, y copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul, o certificado de existencia y representación legal. Cuando se trate de persona extranjera se deberá acreditar el cumplimiento de lo señalado en el libro II titulo XIII del código de comercio y el artículo 48 del

[42] Entidad de Certificación: es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales. (Ley 527)

código de procedimiento civil, según lo dispuesto en el numeral 1 artículo 5 del Decreto 1747 de 2000.

e. Informe de auditoría en los términos del artículo 15 de esta resolución.
f. Estados financieros certificados conforme a la ley y con una antigüedad no superior a seis meses, según lo dispuesto en el numeral 1 del artículo 7 del Decreto 1747 de 2000.
g. Copia del documento que acredite que se han constituido las garantías de acuerdo a lo dispuesto en el artículo 8 del Decreto 1747 de 2000.
h. Documento con descripción detallada de la infraestructura, procedimientos, recursos según lo previsto en el artículo 9 del Decreto 1747 de 2000. El cumplimiento de los requisitos deberá acreditarse según lo previsto en la sección V del Capítulo II de esta resolución.
i. En caso de que la infraestructura sea prestada por un tercero, copia de los contratos o convenios con éstos, en idioma español.
j. Declaración de Prácticas de Certificación, en adelante DPC[43].

---

[43] Artículo 6 del Decreto 1747. La Superintendencia de Industria y Comercio definirá el contenido de la Declaración de Prácticas de Certificación, DPC, la cual deberá incluir, al menos lo siguiente:
1. Identificación de la entidad de certificación.
2. Política de manejo de los certificados.
3. Obligaciones de la entidad y de los suscriptores del certificado y precauciones que deben observar los terceros.
4. Manejo de la información suministrada por los suscriptores.
5. Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.
6. Límites de responsabilidad por el ejercicio de su actividad.
7. Tarifas de expedición y revocación de certificados.
8. Procedimientos de seguridad para el manejo de los siguientes eventos:
   a) cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida;
   b) cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado;
   c) cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio;
   d) cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratados por el suscriptor.
9. El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación.
10. Modelos y minutas de los contratos que utilizarán con los usuarios.
11. Política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

Articulo 19 de la Ley 26.930. Declaración de Prácticas de Certificación. La declaración de prácticas de certificación a que se hace referencia en el artículo 6 del Decreto 1747 de 2000, deberá estar asequible desde el "homepage" de la entidad de certificación, disponible al público en todo momento y tendrá que incluir:
La identificación de la entidad que presta los servicios de certificación. Esta información incluirá el nombre, razón o denominación social de la entidad, el domicilio social, teléfono, fax, dirección de correo electrónico y la oficina responsable de las peticiones, consultas y reclamos de los suscriptores y usuarios. Si la entidad de certificación tiene entidades subordinadas o subcontratadas, deberá incluir esta misma información respecto de cada una de ellas.

La política de manejo de los certificados, que debe incluir:
Los requisitos y el procedimiento de expedición de certificados, incluyendo los procedimientos de identificación del suscriptor y de las entidades reconocidas, de acuerdo con lo previsto en el artículo 43 de la Ley 527 de 1999.
Los tipos de certificados que ofrece, sus diferencias, el grado de confiabilidad y los posibles usos de cada uno de ellos, límites de responsabilidad y el tiempo durante el cual se garantiza la condición de unicidad de la firma digital.
El contenido de cada uno de los distintos tipos de certificados.
El procedimiento para la actualización de la información contenida en los certificados.
El procedimiento, las verificaciones, la oportunidad y las personas que podrán invocar las causales de suspensión o revocación de los certificados.
La vigencia de cada uno de los tipos de certificados.
La Información sobre el sistema de seguridad para proteger la información que se recoge con el fin de expedir los certificados.
Las obligaciones de la entidad de certificación y de los suscriptores del certificado y las precauciones que deben observar los terceros que confían en el certificado.
La información que se le va a solicitar a los suscriptores.
El manejo de la información que se obtiene de los suscriptores de acuerdo a las normas aplicables en la materia, detallando:
El manejo de la información de naturaleza confidencial.
Los eventos en que se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.
Las garantías que ofrece la entidad para el cumplimiento de las obligaciones que se deriven de sus actividades y los clausulados de los seguros que protegen a los terceros por los perjuicios que pueda causar la entidad y/o los reglamentos de los contratos de fiducia constituidos para el efecto.
Los límites de responsabilidad de la entidad de certificación en cada uno de los tipos de certificados y por cada documento firmado.
Las tarifas de expedición y revocación de certificados y los servicios que incluyen.
Los procedimientos de seguridad para el manejo de los siguientes eventos:
Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida.
Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio.

Cambio de servicios ofrecidos en entidad de certificación abierta según la normativa creada bajo la Resolución 26.930**.** Cuando la entidad de certificación abierta pretenda ofrecer nuevos servicios, deberá solicitar autorización previa ante esta Superintendencia, mediante el diligenciamiento del Anexo 4, adjuntando el informe de auditoría correspondiente al nuevo servicio.

De conformidad con el Decreto 1747, la acreditación de requisitos de las entidades de certificación cerradas es regulada de la siguiente manera: quienes pretendan realizar las actividades propias de las entidades de certificación cerradas deberán acreditar ante la Superintendencia de Industria y Comercio que:

a. los administradores y representantes legales no están incursos en las causales de inhabilidad previstas en la Ley 527, y
b. están en capacidad de cumplir los estándares mínimos que fije la Superintendencia de Industria y Comercio de acuerdo a los servicios ofrecidos.

Acreditación de requisitos de las entidades de certificación abiertas. El Decreto 1747, dispone que quienes pretendan realizar las actividades propias de las entidades de certificación abiertas deberán particularizarlas y acreditar ante la Superintendencia de Industria y Comercio:

a. Personería jurídica o condición de notario o cónsul.
b. Cuando se trate de una entidad extranjera, se deberá acreditar el cumplimiento de los requisitos contemplados en el libro segundo, título VIII del Código de Comercio para las sociedades extranjeras que pretendan ejecutar negocios permanentes en territorio colombiano. Igualmente deberá observarse lo establecido en el artículo 48 del Código de Procedimiento Civil.
c. Que los administradores y representantes legales no están incursos en las causales de inhabilidad previstas en la Ley 527.
d. Declaración de Prácticas de Certificación (DPC) satisfactoria, de acuerdo con los requisitos establecidos por la Superintendencia de Industria y Comercio.
e. Patrimonio mínimo de 400 salarios mínimos mensuales legales vigentes al momento de la autorización.
f. Constitución de las garantías previstas en este decreto.
g. Infraestructura y recursos por lo menos en la forma exigida en el artículo 9° de este decreto.
h. Informe inicial de auditoría satisfactorio a juicio de la misma Superintendencia.
i. Un mecanismo de ejecución inmediata para revocar los certificados digitales expedidos a los suscriptores, a petición de éstos o cuando se tenga indicios de que ha ocurrido alguno de los eventos previstos en la Ley 527.

La Superintendencia de Industria y Comercio tendrá la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente.

Si se solicita autorización para certificaciones recíprocas, se deberán acreditar adicionalmente la entidad reconocida, los certificados reconocidos, el tipo de certificados al cual se remite, la vigencia y los términos del reconocimiento.

Patrimonio mínimo. Para determinar el patrimonio mínimo, sólo se tomarán en cuenta las cuentas patrimoniales de capital suscrito y pagado, reserva legal, superávit por prima en colocación de acciones y se deducirán las pérdidas acumuladas y las del ejercicio en curso, conforme a lo estipulado en el Decreto 1747.

El patrimonio mínimo deberá acreditarse:

a. En el caso de personas jurídicas, por medio de estados financieros, con una antigüedad no superior a 6 meses, certificados por el representante legal y el revisor fiscal si lo hubiere.
b. Tratándose de entidades públicas, por medio del proyecto de gastos y de inversión que generará la actividad de certificación, conjuntamente con los certificados de disponibilidad presupuestal que acrediten la apropiación de recursos para dicho fin.
c. Para las sucursales de entidades extranjeras, por medio del capital asignado.
d. En el caso de los notarios y cónsules, por medio de los recursos dedicados exclusivamente a la actividad de entidad de certificación.

Modelos y minutas de los contratos que utilizará. En caso de prever su existencia, texto de las cláusulas compromisorias que establezcan el procedimiento jurídico para la resolución de conflictos, especificando al menos la jurisdicción y ley aplicable en el caso en que alguna de las partes no tenga domicilio en el territorio colombiano.

La política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

Garantías según el Decreto 1747. La entidad debe contar con al menos una de las siguientes garantías:

1. Seguros vigentes que cumplan con los siguientes requisitos:

a. ser expedidos por una entidad aseguradora autorizada para operar en Colombia. En caso de no ser posible lo anterior, por una entidad aseguradora del exterior que cuente con la autorización previa de la Superintendencia Bancaria;
b. cubrir todos los perjuicios contractuales y extra-contractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita autorización o cuenta con autorización;
c. cubrir los anteriores riesgos por una cuantía asegurada por evento igual o superior al mayor entre: i. 7.500 salarios mínimos mensuales legales por evento; o ii. El límite de responsabilidad definido en las prácticas de certificación;
d. incluir cláusula de restitución automática del valor asegurado;
e. incluir una cláusula que obligue a la entidad aseguradora a informar previamente a la Superintendencia de Industria y Comercio la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

2. Contrato de fiducia con patrimonio autónomo que cumpla con las siguientes características:

a. tener como objeto exclusivo el cubrimiento de las pérdidas sufridas por los suscriptores y terceros de buena fe exentos de culpa, que se deriven de los errores y omisiones o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita o cuenta con autorización;
b. contar con recursos suficientes para cubrir pérdidas por una cuantía por evento igual o superior al mayor entre: i. 7.500 salarios mínimos mensuales legales por evento; o ii. El límite de responsabilidad definido en las prácticas de certificación;
c. que los fideicomitentes se obliguen a restituir los recursos de la fiducia en caso de una reclamación, por lo menos hasta el monto mínimo exigido en el punto anterior;
d. que la fiduciaria se obligue a obtener permiso de la Superintendencia de Industria y Comercio, previamente a cualquier cambio en los reglamentos, disminución en el monto o alcance de la cobertura, así como para el retiro de fideicomitentes y para la terminación del contrato;
e. que las inversiones estén representadas en títulos de renta fija, alta seguridad y liquidez emitidos o garantizados por la Nación, el Banco de la República o calificados como de mínimo riesgo por las sociedades calificadoras de riesgo;
f. la entidad que pretenda otorgar el reconocimiento recíproco, deberá acreditar la cobertura de las garantías requeridas en este decreto para los perjuicios que puedan causar los certificados reconocidos.

Conforme al Decreto 1747, en desarrollo de lo previsto en la Ley 527 de 1999, la entidad deberá contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad, tales que:

a. Puedan generar las firmas digitales propias y todos los servicios para los que soliciten autorización.
b. Se garantice el cumplimiento de lo previsto en la Declaración de Prácticas de Certificación (DPC).
c. Se pueda calificar el sistema como confiable de acuerdo con lo señalado en el decreto.
d. Los certificados expedidos por las entidades de certificación cumplan con: d.1) Lo previsto en la Ley 527; y d.2) Alguno de los estándares de certificados que admita de manera general la Superintendencia de Industria y Comercio.
e. Se garantice la existencia de sistemas de seguridad física en sus instalaciones, un monitoreo permanente de toda su planta física, y acceso restringido a los equipos que manejan los sistemas de operación de la entidad.
f. El manejo de la clave privada de la entidad esté sometido a un procedimiento propio de seguridad que evite el acceso físico o de otra índole a la misma, a personal no autorizado.
g. Cuente con un registro de todas las transacciones realizadas, que permita identificar el autor de cada una de las operaciones.
h. Los sistemas que cumplan las funciones de certificación sólo sean utilizados con ese propósito y por lo tanto no puedan realizar ninguna otra función.

i. Todos los sistemas que participen directa o indirectamente en la función de certificación están protegidos por sistemas y procedimientos de autenticación y seguridad de alto nivel de protección, que deben ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación del servicio.

ECUADOR – De acuerdo con lo pautado en la nueva Ley de Comercio Electrónico, las entidades de Certificación de Información son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta Ley y el Reglamento que deberá expedir el Presidente de la República.

La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información. El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

PERÚ –De conformidad con el Reglamento de Ley 27.269, las entidades de certificación[44] acreditadas o reconocidas deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y en el Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Las entidades que soliciten su acreditación como entidades de certificación ante la autoridad administrativa competente deben contar con los elementos de la Infraestructura Oficial de Firma Digital señalados en el Reglamento, y someterse al procedimiento de evaluación comprendido en el Reglamento.

Cuando alguno de los elementos señalados en el párrafo precedente sea administrado por un tercero, la entidad solicitante deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones, y la disponibilidad de estos elementos para la evaluación y supervisión que la autoridad administrativa competente considere necesarias. La autoridad administrativa competente, de ser el caso, precisará los términos bajo los cuales se rigen estos supuestos del servicio de certificación.

La solicitud de acreditación de entidades de certificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:

a. Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.
b. Acreditar domicilio en el país.
c. Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
d. Declaración de prácticas de certificación y documentación que comprenda el sistema de gestión implementado conforme al Reglamento.
e. Declaración jurada del cumplimiento de los requisitos señalados en el Reglamento; información que será comprobada por la autoridad administrativa competente.
f. Documentación que acredite el cumplimiento de lo dispuesto en el Reglamento y demás que la autoridad administrativa competente señale.
g. Informe favorable de la entidad sectorial correspondiente, cuando lo solicite la autoridad administrativa competente, para el caso de las personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.

[44] Entidad de certificación : Persona jurídica que presta servicios de emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación. (Reglamento de la Ley 27.269)

VENEZUELA - Requisitos para ser Proveedor de conformidad con lo estipulado en el Decreto-Ley. Podrán ser Proveedores de Servicios de Certificación[46], las personas, que cumplan y mantengan los siguientes requisitos:

a. La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.
b. La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos. Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.
c. 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, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.
d. Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación.
e. En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.
f. Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.
g. Las demás que señale el reglamento de este Decreto-Ley.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

De la acreditación. El Decreto-Ley establece que los Proveedores de Servicios de Certificación presentarán ante la Superintendencia de Servicios de Certificación Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en la Ley. La Superintendencia de Servicios de Certificación Electrónica, previa verificación de tales documentos, procederá a recibir y procesar dicha solicitud y deberá pronunciarse sobre la acreditación del Proveedor de Servicios de Certificación, dentro de los veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud.

Una vez aprobada la solicitud del Proveedor de Servicios de Certificación, éste presentará, a los fines de su acreditación, garantías que cumplan con los siguientes requisitos:

a. Ser expedidas por una entidad aseguradora o bancaria autorizada para operar en el país, conforme a las disposiciones que rigen la materia.
b. Cubrir todos los perjuicios contractuales y extra-contractuales de los signatarios y terceros de buena fe derivados de actuaciones dolosas, culposas u omisiones atribuibles a los administradores, representantes legales o empleados del Proveedor de Servicios de Certificación.

El Proveedor de Servicios de Certificación deberá mantener vigente la garantía aquí solicitada por el tiempo de vigencia de su acreditación. El incumplimiento de este requisito dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica.

Negativa de la acreditación según el Decreto-Ley. La Superintendencia de Servicios de Certificación Electrónica podrá negar la solicitud a que se refiere el artículo anterior, en caso de que el solicitante no reúna los requisitos señalados en este Decreto-Ley y sus reglamentos.

Sin limitación de otros que se constituyan, el Estado creará un Proveedor de Servicios de Certificación de carácter público, conforme a las normas del presente Decreto-Ley.

[46] Proveedor de Servicios de Certificación: Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley.

Semejanzas y Diferencias: comentarios.

- ***¿Quién puede convertirse en entidad o proveedor de servicios de certificación de conformidad con la normativa antes señalada?***
  En Colombia, las personas jurídicas de carácter público o privado, nacionales o extranjeras, las Cámaras de Comercio, los Notarios y los Cónsules podrán ser entidades de certificación "abiertas". Las entidades públicas, los Notarios y Cónsules podrán ser entidades de certificación "cerradas".[47]

  Las entidades extranjeras deberán acreditar el cumplimiento de determinados requisitos para sociedades extranjeras, que pretendan ejecutar negocios permanentes en territorio colombiano, previstos en el Código de Comercio y el Código de Procedimiento Civil colombianos.

  En Ecuador, las empresas unipersonales y las personas jurídicas podrán ser entidades de certificación de información.

  En Perú, solo las personas jurídicas domiciliadas en Perú podrán ser entidades de certificación. (norma similar a la colombiana)

  En Venezuela las personas (sin ninguna especificación) podrán ser proveedores de servicios de certificación. Dicho país, en una de sus disposiciones legales hace referencia a "organismos públicos y privados" quienes podrán prestar los servicios antes mencionados. Dada la lectura de la normativa venezolana, podemos deducir que las personas jurídicas, constituidas legalmente en Venezuela o en otro país, puede ser proveedores de servicios de certificación, de conformidad con los principios generales de la libre competencia / concurrencia y no-discriminación.

- ***¿Qué tipo de entidades de certificación pueden constituirse?***
  En Colombia pueden crearse entidades de certificación abiertas y cerradas.
  En Ecuador pueden crease entidades de certificación de información autorizadas.
  En Perú están reconocidas las entidades de certificación acreditadas
  En Venezuela, los proveedores de servicios de certificación deben estar acreditados.

- ***¿Cuáles son los requisitos que deben cumplir las entidades que deseen convertirse en entidad de certificación o prestar servicios de certificación? ¿Pueden las entidades prestar sus servicios utilizando la infraestructura de un tercero?***

  Primeramente nos referiremos a las condiciones reflejadas en los países bajo estudio:
  Colombia, Perú y Venezuela establecen que quien desee convertirse en entidad o proveedor de servicios de certificación deberá contar con capacidad económica y financiera suficiente para prestar los servicios antes citados.

  Colombia, Ecuador y Perú disponen que la entidad de certificación que utilice la infraestructura de un tercero deberá demostrar su vinculación con aquél. El primero de los países, solicita la presentación de una copia de los contratos o convenios, en idioma español, celebrados entre la entidad de certificación y el tercero. Colombia y Perú, solicitan la presentación de la Declaración de Prácticas de Certificación (DPC).

---

[47] De acuerdo con lo deducido de nuestras conversaciones con abogados colombianos, explicaremos a continuación, de manera muy simple qué son entidades de certificación abiertas y cerradas en Colombia. Se entiende por entidad de certificación abierta (ECA) aquella entidad que ha sido debidamente acreditada por la Superintendencia de Industria y Comercio (SIC) para prestar servicios de certificación digital al público. Los certificados emitidos por una ECA gozan de plena validez y eficacia jurídica (están plenamente reconocidos en la Ley de comercio electrónico) y son reconocidos públicamente. Si surge un problema y el mismo es llevado ante los tribunales nacionales, el titular del certificado digital no tendrá que probar la validez de su certificado.
Por el contrario, la entidad de certificación cerrada (ECC) puede o no estar acreditada por la SIC para prestar este tipo de servicios. Quien posea un certificado digital emitido por una entidad cerrada (autorizada o no por la SIC) y desee hacer valer su certificado ante un tribunal, deberá soportar la carga de la prueba, es decir, que tendrá que probar que el certificado ha sido emitido de conformidad con los estándares internacionales y un perito especialista en la materia deberá intervenir durante el transcurso del litigio para comprobar la veracidad del dicho del titular del certificado. Las ECC fueron creadas para prestar servicios de certificación a "comunidades cerradas" a "núcleos privados". Por ejemplo: certificados emitidos únicamente a los empleados (y demás personas que mantenga una relación comercial con la empresa) de una empresa para ser usados en el intercambio de mensajes de datos dentro de la empresa. Esto se aplica a toda entidad de certificación cerrada dentro y fuera de Colombia. (Aconsejamos leer con detenimiento las normas sobre entidades de certificación en estudio para obtener una mejor comprensión sobre el tema)

Colombia y Venezuela adoptaron condiciones similares a ser cubiertas por quien busque convertirse en entidad o proveedor de servicios de certificación. Ellas, son las siguientes: contar con capacidad y elementos técnicos necesarios para proveer certificados electrónicos y garantizar un mecanismo de ejecución inmediata de revocación de los certificados digitales. Ambos países estipulan que las entidades o proveedores de servicios de certificación deben contar con las garantías que citamos a continuación:

a. ser expedidos por una entidad aseguradora autorizada para operar en Colombia. En caso de no ser posible lo anterior, por una entidad aseguradora del exterior que cuente con la autorización previa de la Superintendencia Bancaria; y
b. cubrir todos los perjuicios contractuales y extra-contractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita autorización o cuenta con autorización.

En segundo lugar, consideramos pertinente, hacer mención de todos los requisitos restrictivos, que limitarán enormemente el número de entidades de certificación que logren obtener la debida autorización para ejercer su actividad:
- para convertirse en entidad de certificación abierta en Colombia, aquélla debe demostrar que la actividad en cuestión está prevista en su objeto social principal.

Nos parece subjetiva la evaluación de la condición prevista en la Ley colombiana, que indica que las entidades de certificación deben acreditar ante la Superintendencia de Industria y Comercio un informe inicial de auditoría "*satisfactorio a juicio de la misma Superintendencia*".

- ***¿Ante qué autoridad debe solicitarse autorización o acreditación para tal fin?***

El órgano regulador de las entidades de certificación en Colombia es la Superintendencia de Industria y Comercio adscrita al Ministerio de Desarrollo Económico de Colombia.

El órgano de regulación de las entidades de certificación de información es, en Ecuador, el Consejo Nacional de Telecomunicaciones (CONATEL) y el órgano de control es la Superintendencia de Telecomunicaciones.

En Perú, la Autoridad Administrativa competente que acreditará las entidades de certificación es el Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual (INDECOPI).

En Venezuela, la Superintendencia de Servicios de Certificación Electrónica, adscrita al Ministerio de Ciencia y Tecnología, es el órgano que acredita a las entidades o proveedores de servicios de certificación.

Recomendación.

Podemos concluir esta parte del trabajo, aconsejando que las normas que sean elaboradas con la finalidad de regular, entre otros, la creación, acreditación, requisitos, funciones y las obligaciones de las entidades de certificación, traten en lo posible de salvaguardar el objetivo y el espíritu de tales normas. Es decir, que se concentren en tratar de establecer garantías legales y seguridad jurídica a todo lo que se encuentre relacionado con los servicios de certificación.

También sugerimos, que la normativa se fundamente en los principios generales de libre concurrencia o competencia y en la no-discriminación. Nos referimos, particularmente, a la cantidad de requisitos adicionales exigidos a entidades de certificación extranjeras para operar en uno de los países de la subregión andina. Asimismo, recomendamos, reconocer la necesidad, viabilidad y existencia de entidades de certificación creadas utilizando tecnología e infraestructura de un tercero (por ejemplo: una entidad de certificación nacional o extranjera).

Las entidades de certificación, no son un negocio, son una necesidad planteada por la falta de seguridad en las transacciones electrónicas.

D. Entidades / Autoridades de Certificación y Registro:

2. Entidades de Registro

La figura de la entidad de registro es poco conocida. Generalmente, se desconoce su existencia, y cuando se la conoce, se ignora su importante función dentro del esquema de las entidades de certificación y, concretamente, en la prestación de servicios de certificación. Por esta razón, compartiremos con el lector, extractos de un trabajo sobre "Transacciones seguras" realizado por el Sr. Luciano Moreno (BJS Software)[48].

Se hace imperativo, hacer referencia a los certificados *Secure Electronic Transactions* (SET)[49], ya que los mismos "se estructuran siguiendo una jerarquía piramidal única, cuya cúspide es ocupada por la Entidad Certificadora Raíz (Root CA), que es la encargada de certificar a todas las demás entidades certificadoras".

Bajo esta Root CA "se encuentran las Entidades de Certificación de Marca (Brand CA) encargadas, principalmente, de emitir certificados SET a Entidades de Certificación Final (Geopolitical CA)." "Las Brand CA pueden, a su vez, autorizar estas últimas, para que funcionen como entidades certificadoras, quienes tendrán la tarea de emitir los certificados SET a los usuarios finales".

"A la hora de obtener un certificado SET se requiere un proceso de autentificación de los datos que en él van a figurar, al igual que sucede con los certificados UIT-T X.509 v3." "En el caso de SET la verificación de datos corresponde a unas entidades creadas al efecto, que se denominan Entidades de Registro, cuya labor es la de actuar como avaladoras ante la Entidad de Certificación (EC) de los usuarios que solicitan el certificado, encargándose también de tramitar los mismos."

"Las Entidades de Registro actúan en nombre y por cuenta de la EC correspondiente. Sus principales misiones son: validar solicitudes de certificado en base a determinados procedimientos de identificación, según el tipo de certificado; solicitar luego el correspondiente certificado a la EC; y, una vez obtenido, entregar el mismo al usuario final."

"Toda Entidad de Registro debe tener, a disposición de los solicitantes, una Declaración de Prácticas de Registro, que especifique claramente los procedimientos operativos y de garantía de seguridad que exige y facilita." (Observaremos que el Reglamento a la Ley Peruana de firmas y certificados digitales, prevé esta disposición dentro su articulado.)

La *Entidad de Registro* es una figura que aparece raramente en las legislaciones nacionales sobre comercio electrónico que incluyen las entidades de certificación dentro de su objetivo y ámbito de aplicación. Afortunadamente, uno de los Países Miembros de la Comunidad Andina la ha previsto dentro de su derecho interno. Por este motivo, pasaremos a citar la norma en cuestión.

Es de importancia capital, acoger en futuras legislaciones o en una Decisión comunitaria, el principio de la libre competencia con respecto a las entidades de certificación y registro, tal como lo hace el Reglamento peruano al establecer que LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ASÍ COMO LOS DE REGISTRO O VERIFICACIÓN SE REALIZA EN EL **RÉGIMEN DE LIBRE COMPETENCIA**.

BOLIVIA - No posee disposiciones legales que traten este tema.

COLOMBIA - No posee disposiciones legales que traten este tema.

ECUADOR - No posee disposiciones legales que traten este tema.

---

[48] El texto de este documento ha sido reproducido con la debida autorización emitida por su autor, vía e-mail, en fecha 24 de abril de 2002. Las comillas reflejan las partes del artículo que fueron transcritas en el presente trabajo.

[49] "En febrero de 1996 un grupo de empresas del sector financiero, informático y de seguridad (Visa *International*, MasterCard, Microsoft, Nestcape, IBM, RSA, etc.) anunciaron el desarrollo de una nueva tecnología común destinada a proteger la compras a través de redes abiertas como Internet basadas en el uso de tarjetas de crédito. Esta nueva tecnología se conoce con el nombre de *Secure Electronic Transactions* (Transacciones Electrónicas Seguras), SET, y ha sido creada exclusivamente para la realización de comercio electrónico usando tarjetas de crédito. SET se basa en el uso de certificados digitales para asegurar la perfecta identificación de todas aquellas partes que intervienen en una transacción *online* basada en el uso de tarjetas de pago, y en el uso de sistemas criptográficos de clave pública para proteger el envío de los datos sensibles en su viaje entre los diferentes servidores que participan en el proceso." Texto extraído del trabajo "Transacciones seguras (X)", Luciano Moreno Departamento de diseño web de BJS Software, URL: http://www.htmlweb.net/seguridad/ssl/ssl_10.html

PERÚ– De conformidad con la DEFINICIÓN del novedoso y reciente Reglamento de la Ley 27.269 peruana, la Entidad de Registro es una persona jurídica encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la identificación y autenticación del suscriptor de una firma digital, la aceptación y autorización de las solicitudes para la emisión y modificación de certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

La Ley 27.269 estipula que la Entidad de Registro o Verificación cumple con la FUNCIÓN de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Las entidades de registro o verificación acreditadas tienen las siguientes OBLIGACIONES, de conformidad con el Reglamento de la Ley:

a) Cumplir los procedimientos declarados para la prestación del servicio.
b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante de certificado digital bajo responsabilidad.
c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.
d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
e) Informar y solicitar autorización a la autoridad administrativa, especialmente en el supuesto previsto en el artículo 48º del Reglamento.
f) Acreditar domicilio en el Perú.
g) Contratar los seguros necesarios que le permitan indemnizar por los daños que puedan ocasionar como resultado de las actividades de registro o verificación.

El Reglamento a la Ley 27.269, prevé que las entidades que soliciten su acreditación como entidades de registro o verificación ante la autoridad administrativa competente deben contar con procedimientos para la prestación de sus servicios, los mismos que tendrán que asegurar la verificación directa de la identidad del solicitante. Toda entidad de registro y/o verificación debe contar, además, con un respaldo financiero.

Este reglamento regula también el CESE DE LAS OPERACIONES de dichas entidades e identifica las causales que dan lugar al ello:

a) por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión;
b) por extinción de su personería jurídica;
c) por revocación de su registro;
d) por sanción dispuesta por la autoridad administrativa competente;
e) por orden judicial;
f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contenidos en los incisos a) y b), la entidad de registro o verificación debe notificar el cese de sus actividades a la autoridad administrativa competente con una anticipación mínima que será establecida por ésta, debiendo dejar constancia ante aquélla de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el Reglamento.

VENEZUELA - No posee disposiciones legales que traten este tema.

Comentarios.

En vista del vacío existente en cuanto a una definición de las entidades de registro, consideramos apropiado remitirnos a textos legales o proyectos de Ley y/o reglamento adoptados por otros países latinoamericanos, no miembros de la subregión. A título puramente informativo, decidimos transcribir la normativa argentina que regula las entidades de registro. Éste no es más que un ejemplo entre otros, de legislaciones nacionales que han adoptado la figura de la entidad de registro.

El Ante-proyecto de Reglamento de Ley argentina establece que los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación.

Conforme a lo pautado en este anteproyecto, una Autoridad de Registro es una entidad responsable de las siguientes funciones:

1. La recepción de las solicitudes de emisión de certificados;
2. La validación de la identidad y autenticación de los datos de los titulares de certificados;
3. La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado;
4. La remisión de las solicitudes aprobadas al Certificador Licenciado[50] con la que se encuentre operativamente vinculada;
5. La recepción y validación de las solicitudes de revocación de certificados, y su direccionamiento al Certificador Licenciado con el que se vinculen;
6. La identificación y autenticación de los solicitantes de revocación de certificados;
7. El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado;
8. Cumplir las normas y recaudos establecidos para la protección de datos personales;
9. El cumplimiento de las disposiciones que establezca la Política de Certificación y, el
10. Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

[50] El Certificador Licenciado es el equivalente a Entidad o Proveedor de Servicios de Certificación Acreditado.

Conclusiones

Para que tenga lugar una uniformidad internacional satisfactoria de las normas sobre comercio electrónico y áreas conexas, debemos empezar esta ardua tarea por la elaboración de una armonización regional (comprendidas las subregiones). Las Directivas Europeas y los principios generales del UNIDROIT, las Leyes Modelo de la UNCITRAL y las recomendaciones de la Organización de Cooperación y Desarrollo Económico (OCDE) o de la UIT, son la prueba de lo antes afirmado.

Este trabajo no ha pretendido ser exhaustivo y su contenido no debe ser considerado, en ningún caso, como una premisa o principio elaborado por la UIT; sin embargo consideramos que nuestros consejos, sugerencias, comentarios y recomendaciones están en armonía con la tendencia internacional en materia de comercio electrónico. Recordamos, que los temas no tratados en el presente reporte, serán abordados en un segundo reporte previsto para el segundo semestre de 2002.

Esperamos que este estudio haya proporcionado suficiente información para dar a conocer la situación actual del marco jurídico del comercio electrónico y contribuido al intercambio de la misma entre los países de la subregión en materias de mensajes de datos, de firmas electrónicas (y digitales), de certificados digitales y de entidades y/o proveedores de servicios de certificación y registro.

Es muy alentador, comprobar que la legislación y proyectos de ley y/o reglamentos existentes en torno al comercio electrónico en la subregión andina están *quasi* a la par con la *Lex Mercatoria*[51] (y otras fuentes de derecho internacional) y esperamos que una Decisión comunitaria sea adoptada siguiendo, tanto las disposiciones nacionales innovadoras y plausibles como los lineamientos pautados por la opinión internacional y reflejados en el ordenamiento jurídico de los países que encabezan la fila de Naciones que, hoy, gozan de los beneficios del comercio electrónico en su totalidad. La brecha digital existente en el ámbito legal ha sido disminuida, esperamos que el mismo evento se produzca en la práctica.

Sabemos que hay mucho camino por recorrer para obtener un conjunto de normas uniformes sobre comercio electrónico y, que si bien es cierto, que identificamos algunas semejanzas entre las legislaciones nacionales de los cinco países de la subregión; no es menos cierto, que existen muchas disparidades entre las mismas. Lo importante, ahora, es emprender ese camino.

Existe la voluntad política de los Países Miembros de la Comunidad Andina para acoger una norma supra-nacional sobre comercio electrónico y la Secretaría General de la Comunidad Andina de Naciones tiene el mandato de preparar una Decisión en este sentido. Esperamos que el estudio y análisis aquí contenidos sean de utilidad para esa Secretaría, en el proceso de redacción del proyecto de Decisión que será sometido a los países correspondientes.

Este proceso de armonización del marco legal del comercio electrónico facilitará, mejorará y, posiblemente, aumentará, las relaciones comerciales entre los países signatarios del Acuerdo de Cartagena, y abrirá una puerta adicional hacia, el tan ansiado, Mercado Común Andino.

[51] A pesar de las críticas, ésta figura es de uso corriente en derecho de comercio (o derecho mercantil) internacional, particularmente, en arbitrajes y contratos internacionales. La *Lex Mercatoria* engloba los usos y costumbres del comercio internacional, inclusive, los principios transnacionales. Berthold Goldman, profesor de la Universidad de Derecho, Economía y Ciencias Sociales de Paris - Francia afirma que la *Lex Mercatoria* está compuesta de reglas materiales aptas a gobernar las relaciones económicas internacionales. (Goldman, Berthold, DOCTRINE – 'La *lex mercatoria* dans les contrats et l'arbitrage internationaux : réalité et perspectives", Journal du Droit International, No. 106e année, No. 1, Janvier – Février - Mars, Editions Techniques S.A., Paris, 1979, páginas 475 - 505).

Bibliografía

A. Artículos

- Arguedas, Ysella, Analista Legal, Instituto Peruano de Comercio Electrónico (IPCE), "El tema de Firmas y Certificados Digitales en el Perú". pp. 20. URL: http://www.ipce.org.pe/firmas.htm

- Benabou, Valérie Laure, Profesora, Universidad de Lyon 2, *« Faut-il une harmonisation minimale du droit? ». Colloque International sur le Droit de l'Internet - Approches européennes et internationales, 19-20 novembre 2001, Assemblée Nationale, Liste des Contributions Reçues*. URL: http://droit-internet-2001.univ-paris1.fr/vf/page004.html

- Goldman, Berthold, DOCTRINE – "La *lex mercatoria* dans les contrats et l'arbitrage internationaux: réalité et perspectives", Journal du Droit International, No. 106e année, No. 1, Janvier – Février - Mars, Editions Techniques S.A., Paris, 1979, páginas 475 – 505.

- IDC, "El miedo al fraude es el principal obstáculo para el desarrollo de Internet en América Latina" Publicado en la página web : MasterNet.com. URL: http://www.masterdisseny.com/master-net/atrasadas/104.php3

- Rueda Garcés, Pedro Nel. "Comparación detallada entre la Ley 527 Colombiana de 1999 y la Ley Modelo de la CNUDMI: Artículo por Artículo". pp. 24. URL: http://www.arkhaios.com/ecommerce/comparacion/artxart.htm

- Segura Loarte, Alejandro. "Los órganos de acreditación de los prestadores de servicios de certificación digital en el ordenamiento jurídico peruano y en la legislación comparada". Febrero de 2002. URL: http://democraciadigital.org/etc/arts/0202organos.html

- Segura Loarte, Alejandro. Mensaje electrónico de fecha 27 de febrero de 2002 sobre las autoridades de acreditación de las entidades de prestación de servicios de certificación digital. Comunidad Alfa-REDI.

- Utsumi, Yoshio, Secretario general, Unión Internacional de Telecomunicaciones. "El desarrollo tecnológico no basta". Día Mundial de las Telecomunicaciones. 17 de mayo de 1999.

  URL: http://www.itu.int/newsarchive/wtd/1999/iht05/ecom7-es.html

- Utsumi, Yoshio, Secretario General de la Unión Internacional de Telecomunicaciones. "Mensaje". Día Mundial de las Telecomunicaciones. 17 de mayo de 1999.
  URL: http://www.itu.int/newsarchive/wtd/1999/index-es.html

B. Documentos

- Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (ASETA). Folleto - Presentación.

- Corporación Ecuatoriana de Comercio Electrónico (CORPECE), Análisis sobre el proyecto de ley de comercio-e ecuatoriano. URL: http://www.corpece.org.ec/documentos/ley/analisis_ley_ce.zip

- Laguna Quiroz, Rosa. "Comercio Electrónico: Hacia la Armonización de Políticas y Regulación Andina". "Marco Regulatorio para el comercio electrónico". 20-21 Nov. 2001. Cochabamba, Bolivia. pp. 21. URL: http://www.comunidadesweb.com/ca/psg?vista_serv=18&tofolder=1851

- Martín Reyes, María de los Ángeles, Profesora Titular de Derecho Mercantil de la Facultad de Derecho de la Universidad de Málaga. Técnico de Administración General del Excmo. Ayuntamiento de Málaga, en excedencia. Miembro del Grupo EUMEDNET de Investigación del Comercio electrónico en las PYMES andaluzas. "Las Entidades de Certificación. Área Premium Nuevas Tecnologías". No. 35, vid:1.107936.3. pp. 8. Documento impreso en fecha 09 de enero de 2002. URL: http://v2.vlex.com/es/premium/print.asp?Articulo=107936

- Moreno Cerro, Luciano, Departamento de diseño web, BJS Software S.L., "Transacciones seguras". Capítulos IX y X. Artículos sobre Seguridad. HTMLWeb. Madrid - España, URL: http://www.htmlweb.net/seguridad/ssl/ssl_10.html

- Muñoz Esquivel, Oliver, Licenciado en Derecho y Ciencias Políticas por la Universidad de Panamá y *Master of Laws in International Trade Law* por la Universidad de Arizona. "Actividad de las Entidades de Certificación Frente a la Función Notarial". No. 35, vid:1.107945.3. pp. 3. Documento impreso en fecha 09 de enero de 2002. URL: http://v2.vlex.com/es/premium/print.asp?Articulo=107945

- *The Economist. The EIU ebusiness forum. The Economist Intelligence Unit (EIU).* "*Pyramid Research e-readiness rankings*" Fecha: 8 de mayo de 2001. URL: http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=367&country_id=PL&channelid=6&categoryid=20&title=Introducing+the+EIU%27s+e%2Dbusiness%2Dreadiness+rankings+World

- Unión internacional de Telecomunicaciones. Documento de discusión titulado "Consideraciones de política en relación con el comercio electrónico" presentado durante el Día Mundial de las Telecomunicaciones del 17 de mayo de 1999. URL: http://www.itu.int/newsarchive/wtd/1999/dp-es.html

- *WISeKey Public Key Infrastructure. "White Paper on the Deployment of Affiliate Registration Organizations (Bronze Service Provider)".* Versión 1.0. Agosto de 2001. URL: http://www.wisekey.com/bronzelevel.htm

C. Legislación (incluye proyectos de Ley y/o reglamentos) *y Leyes Modelo*

CNUDMI

- Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su Incorporación al Derecho Interno con la adición del Artículo 5 bis en la forma aprobada en 1998. 1996.
  URL: http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm

- Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). Ley Modelo de la CNUDMI sobre Firmas Electrónicas. 2001. URL: http://www.uncitral.org/en-index.htm

BOLIVIA

- Proyecto de: Código de Procedimiento Civil, Código Civil, Ley 12760 de fecha 6 de agosto de 1975; Código Tributario; Ley de Propiedad Intelectual, Código de Comercio. Decreto Ley No. 14379.

- Fuentes: El Sitio Jurídico. Aporte del Lic. Iván Rosales. Páginas de consulta, orientación y links de derecho boliviano. Link; Legislación Boliviana. URL: www.geocities.com/bolilaw/legisla.htm y Laguna Quiroz, Rosa. Ministerio de Justicia y Derechos Humanos. "Comercio Electrónico: Hacia la Armonización de Políticas y Regulación Andina". "Marco Regulatorio para el comercio electrónico". 20-21 de noviembre de 2001. Cochabamba, Bolivia. pp. 21.
  URL: http://www.comunidadesweb.com/ca/psg?vista_serv=18&tofolder=1851

COLOMBIA

- Ley 527 del 18 de agosto de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Fuente: http://rechtsinformatik.jura.uni-sb.de/cbl/statutes/Colombia99.html

- Decreto No. 1.747 del 11 de septiembre de 2000 por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Fuente: http://www.ahciet.net

- Resolución Nº 26.930 del 26 de 10 octubre de 2000 por medio de la cual se fijan los estándares para la autorización y funcionamiento de las Entidades de Certificación y sus Auditores. Fuente: http://www.hfernandezdelpech.com.ar/Internet.htm y http://www.ahciet.net

ECUADOR

- Ley de Comercio Electrónico. http://www.corpece.org.ec

- Veto al nuevo proyecto de Ley. Fuente: http://www.corpece.org.ec

- Nuevo Proyecto de Ley de Comercio Electrónico. Fuente: http://www.corpece.org.ec

- Informe de la Comisión de lo Civil y Penal sobre el Proyecto de Ley de Comercio Electrónico del Ecuador. Fuente: http://www.corpece.org.ec

PERÚ

- Ley No. 27.269 de Firmas y Certificados Digitales Promulgada el 26 de mayo de 2000 y Publicada el 28 de mayo de 2000. Fuente: http://rechtsinformatik.jura.uni-sb.de/cbl/statutes/PERÚ_certificadosdigitales.html

- Ley 27.310 que modifica el artículo 11° de la ley N° 27269. 15 de julio de 2000. Fuente: http://www.inei.gob.pe/inei4/FirmaDigital/ley_n27310.htm

- Proyecto de Reglamento de la Ley 27.269. Fuente: http://www.editoraPERÚ.com.pe/normas/indice.html

- Reglamento de la Ley de Firmas y Certificados Digitales. Decreto Supremo No. 019-2002-JUS. 17 de mayo de 2002. Fuente: www.teleley.com
- Ley No. 27.291 que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica. 23 junio de 2000. Fuente: http://www.hfernandezdelpech.com.ar/Leyes/Ley%2027291%20de%20PERÚ.htm
- Ley 27.419 sobre notificación por correo electrónico del 25 de enero de 2001. Fuente: http://www.ipce.org.pe/leyc.htm
- Resolución 000103 de Aduanas relativa a firmas y certificados digitales. Fuente: http://www.alfa-redi.com/documento/data/28.asp

VENEZUELA

- Decreto 1.024 –Ley sobre Mensajes de Datos y Firmas Electrónicas. 10 de febrero de 2001 Fuente: http://vlex.com/ve/revista/16 y http://www.tsj.gov.ve/legislacion/dmdfe.htm

D. Páginas / Sitios web

- Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (ASETA). URL: http://www.aseta.org/

- Asociación de Entidades de Confianza Digital. URL: http://www.aecodi.org/

- Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCIET). URL: http://www.ahciet.net/pag.asp?pag=negocios/comercio_electronico/default.htm&mnu=negocios/negocios.htm

- Banderas de todos los países. Banderas: de Bolivia, Colombia, Ecuador, Perú y Venezuela. URL: http://www.theodora.com/flags/es/

- Centro De Información sobre Calidad, Seguridad y Medio Ambiente. Link: "Entidades de certificación en España". URL: http://www.cigal.igatel.net/html/cert.htm

- Comunidad Andina de Naciones (CAN). Link: Síntesis de los Debates: Conclusiones y recomendaciones del debate sobre "Comercio electrónico: El negocio del siglo XXI" (Mayo 2000) URL: http://www.comunidadandina.org/debates/sintesis2.htm

- *European Quality Assurance (EQA).* URL: http://www.eqa.es/sistemas_calidad.htm

- *Forest Stewardship Council (FCA)*. "Lista de Entidades de Certificación Acreditadas por el FCA". Documento 5.3.1 de fecha 19 de marzo de 2002. URL: http://www.fscoax.org/html/5-3-1_esp.html y "Lista de Entidades de Certificación Solicitantes de acreditación por parte del FSC". Documento 5.3.2 de fecha 11 de octubre de 2001. URL: http://www.fscoax.org/html/5-3-2_esp.html

- Ministerio de Relaciones Exteriores de Bolivia. Link: Comunidad Andina – Secretaría Pro-Témpore. URL: http://www.rree.gov.bo/protempore/inicio.htm

- *National Geographic. Link: Maps and Geography.* URL: http://www.nationalgeographic.com/maps/index.html

- Red Productos Médico-Sanitarios, *MEDICAL DEVICES NETWORK*. España. Link: "Entidades de Certificación de Sistemas de la Calidad". URL: http://www.m-d-n.com/calidad/ent_cert.htm

- Superintendencia de Industria y Comercio. Bogotá – Colombia. "Entidades Autorizadas para operar en el Territorio Nacional Como Entidades de Certificación para Comercio Electrónico" URL: http://www.sic.gov.co/Informacion%20de%20interes/E-commerce.htm

- *The travel site*. "*Central & South America*". URL: http://www.thetravelsite.com/gSoAm.html

E. Recomendaciones de la UIT-T

- "Recomendación de la UIT-T X.509 (03/2000). Information technology - Open systems interconnection". URL: http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-I

F. Lista de entidades y organismos visitados por la UIT y ASETA en Colombia, Ecuador, Perú y Venezuela.

COLOMBIA:

Carlos **FORERO**, Coordinador, Agenda de Conectividad, Carrera 8 # 12-00 Mez., Telf.3442270 cforero@agenda.gov.co

Hermann **ZUBIETA URIBE**, Asesor Despacho Superintendente, Superintendencia de Industria y Comercio, Carrera 13 No. 27-00 P. 10, Telf. 382 26 56, asesorcomer@sic.gov.co

Maria Clara **GUTIÉRREZ**, Dirección de Integración Económica, Ministerio de Comercio Exterior, Calle 28, No. 134-A-15, Telf. 6067534, mariag@mincomex.gov.co

Fernando **FERNÁNDEZ**, Gerente General, Certicámara, Cra. 9 16-21, A.A. 29824, Telf. 560 0280 – 381 0270 ext. 545, fernando.fernández@certicamara.com www.certicamara.com

Dr. Marco **PÉREZ**, Gerente, Property Rights, Consultores Legales, Carrera 8, No. 64-42, of. 316, Telf. 3492733 / 2487841, propertyrights@sky.net.co www.propertyrights.com.co

Dr. Diego **GARZÓN**, Strategist, Azurian, Carrera 13 No. 93-68, Of. 501, Telf. 640 0020 dgarzon@azurian.com

Dr. Alejandro **SERRANO**

Sr. Alain Bossuet **NIÑO RIAÑO**, Dirección Legal de relaciones con el cliente, Vice-presidencia Jurídica, ETB, Carrera 7 No. 20-56, p.6, Bogotá
Telf. 242 23 12 / 242 23 53
alaininr@etb.com.com

Sr. Juan Pablo **RINCÓN C.**,

Sra. Patricia **PARRA A.**,

Sra. Nancy C. **SERRANO V.**,

Sr. Manuel Antonio **PÉREZ C.**,

Sr. Armando Acuña **MARTÍNEZ**,

Sra. María B. **SANTIS S.**,

Sr. Germán Martín **ESTEBAN D.**,

Sra. María Isabel **DELGADO P.**

Ing. Alberto **GRAJALES**, TELECOM, Calle 23, No. 13-49, Bogotá

Gustavo **PEÑA QUIÑÓNEZ**, Calle 118 Nº 54-29 Int. 1, Bogotá,
Telf. 57(1) 271 2018,
Cel. 57(3) 348 4618
gpenaq@supercabletv.net.co
www.regulatel.org

Gabriel Ernesto **PEÑA RODRÍGUEZ**, Notaría 61, Carrera 62, No. 9ª-40, Bogotá, Telf. 2907001 / 290 7140 notaria61@sky.net.co

Alberto **GUERRERO**, General Director, ETEK Empresas de Seguridad Informática, CALLE 93 A No. 11-48 p.2 Telf. 257 1520 aguerrero@etek.com.co www.etek.com.co

ECUADOR:

Ing. Jairo **GÓMEZ**, Director, Estudios y Proyectos, ASETA, Calle de La Pradera, No. 510, Casilla Postal 171106042, Tel. 00593 22 563 812, jgomez@aseta.org

Ing. Gales **CHIRIBOGA**, Coordinador Sector de las Telecomunicaciones, Consejo Nacional de Modernización del Estado (CONAM), Edif. Corporación Financiera Nacional, p.10, Juan León Mera 130 y Av. Patria, Telf. +593 2 250 5025 / 250 5026
gchiriboga@conam.gov.ec

Dr. José Luis **BARZALLO**, Barzallo & Barzallo Abogados, Colón 535 y Av. 6 de Diciembre, Edif. Cristóbal Colón, 6to. piso, Of. 42, Telf. 00593 2 2528774 / 2544464, joseluis@barzallo.com www.barzallo.com

Dr. Julio **MARTÍNEZ**, Secretario (jmartinez@conatel.gov.ec) y Jaime Rodrigo **NÚÑEZ**, Asesor Jurídico (jnunezburbano@yahoo.com, jaime_rodrigo@yahoo.com), Consejo Nacional de Telecomunicaciones (CONATEL), Funcionarios de la Agenda Conectividad, Av. Diego de Almaro 31-95 y Alpallana, Casilla postal 17-07-9777, Telf. +593 2 2224123 / (09) 9442816,

Dr. Gabriel **RUÍZ**, Presidente y Lcda. Patricia Vayas, Secretaria de la Comisión de lo Civil y lo Penal, Congreso Nacional, Av. 10 de Agosto y Checa, Edif. Pichincha, Telf. 900 200 / 900 365.

Ing. Carlos **VERA QUINTANA**, Presidente, Corporación Ecuatoriana de Comercio Electrónico (CORPECE), Almagro No. 32-349 y Shyris, Quito. Tel. 02 2509 578, info@corpece.net www.corpece.net.ec

Ings. Esteban **MATHEUS** y ZAMBRAN **ABUJAS**, Jefe Técnico ealbuja@andinatel.com, ANDINANET, Jorge Drom y Av.

Gaspar de Villarroel, 1er. Piso, Telf.+593 2 292 42 20

Ing. Verónica **YEROVI**, Superintendencia de Telecomunicaciones, Ave. 9 de Octubre 1645 y Berlín, 9no. Piso, Telf. +593 2 2220785

Sr. Franklin **ZAMBONINO**: fzamboni@server.supertel.gov.ec

Sr. Franklin **CONDOR**: fcondor@server.supertel.gov.ec

Sr. Crystian **DIAZ**: cdiaz@server.supertel.gov.ec

Sra. Isabel **LUNA**: iluna@server.supertel.gov.ec

Sr. Iván **ROSSERO**: irosero@server.supertel.gov.ec

Sra. Aída **VASCONEZ**: avascone@server.supertel.gov.ec

Sra. Melba **AGUIRRE**: maguirre@server.supertel.gov.ec

Sr. Gustavo **GUERRA**: gguerra@server.supertel.gov.ec

Sr. Alonso **LLANOS**: allanos@server.supertel.gov.ec

Dr. Andrés **DONOSO**, Vice-presidente de asuntos regulatorios y legales, Bellsouth, Otecel SA, Av. Republica y La Pradera Esq. Quito, Casilla 1717792, Telf. 227700 Ext. 2902 / 227 824 adonoso@bellsouth.com.ec

Dra. Evelyn **LÓPEZ DE SÁNCHEZ**, Corral Sánchez abogados, Av. Republica de El Salvador No. 880, Edif. Almirante Colón, 8vo. Piso, Quito, Telf. 469300 / 469301, corsan_abg@accessinter.net

Dr. Fernando **FERRO ALBORNOZ**, Gerente de Asuntos Regulatorios, Bellsouth, Otecel SA, Av. Republica y La Pradera Esq. Quito, Casilla 1717792, Telf. 227700 Ext. 2903 / 227 824 fferro@bellsouth.com.ec

Dr. Federico **CHIRIBOGA**, OCETEL SA, Asesor externo, fchiriboga@pbplaw.com

Ab. Gabriela **ZUÑIGA**, OCETEL SA, gzuniga@bellsouth.com.ec

Ab. Blanca Isabel **EGAS**, Asesor Legal, OCETEL SA, iegas@bellsouth.com.ec

Abg. R. **ZAMBRANO**, rzambrano@bellsouth.com.ec

Ing. José **VANONI**, Jefe Unidad de Sistemas, PetroEcuador, Alpallana E-8-86 y Av. 6 de Dic., PO Box 17-11-5007, Quito, Telf. 524737 / 524072 jvanoni@petroecuador.com.ec

Dr. Roberto **PONCE**, Embajador, Director General de la Unidad ALCA – Ecuador, Ministerio de Relaciones Exteriores, Carrión y 10 de Agosto, 3er p., Quito Tel. 2220198;

Econ. Herlinda **SABANDO M**, Dirección de Negociaciones Internacionales, Min. De Comercio Exterior, Industrialización, Pesca y Competitividad (MICIP), Edif. Ministerio de Agricultura (MAG), Av. Eloy Alfaro y Amazonas, 2do. P., Tel. 2548980 / 2523261; comercio8@micip.gov.ec hsabando@hotmail.com

Germán **ORTEGA**, Sub-Secretario de Comercio exterior e integración, MICIP, Edif. Ministerio de Agricultura (MAG), Av. Eloy Alfaro y Amazonas, 2do. P., Casilla 12-03-194-A, Telf. 2566784 comercio1@micip.gov.ec

Dip. Ing. Julio **NOVOA**, Diputado por la Provincia de Pichincha, Congreso, Piedrahita, Mez., Escolta Legislativa, of. M16, Tel. 900211

PERÚ:

Dr. Jorge **MUÑIZ ZICHEZ**, Muñiz, Forsyth, Ramírez, Pérez-Taiman & Luna-Victoria Abogados, Las Begonias 475, 6to. Piso, Lima 27, Telf. 51 1 611 7001 / 611 7000 www.munizlaw.com jmuniz@munizlaw.com

Ing. Víctor **PEREYRA**, Servicios de Comercio Electrónico pereyra@limatel.net

Ing. Eduardo Escardo, Presidente Ejecutivo, otros LIMATEL, Av. Camino Real 111, Of. 205, Lima 27, Telf. +511 441 4444, limatel@attmail.com www.limatel.com.pe y www.limatel.net

Dra. Maria Eugenia **DANGOND**, Gerente de Proyectos de Comercio-e, Secretaria General de la Comunidad Andina (CAN), Paseo de la Republica 3895, San Isidro, Telf. +511 4111400 mdangond@comunidadandina.org www.comunidadandina.org

Dr. Carlos Enrique **BECERRA**, Decano del Colegio de Notarios del Perú, Notaria, Chichón 601 en San Isidro, Telf. 4220097 y 4221372 notarius@amauta.rcp.net.pe y Colegio de Notarios, Av. Gregorio Escobedo 343, J. Marta, Telf. 4610016 / 4611150

Dra. Hortensia **ROSAS**, Telefónica del Perú, Av. Arequipa 1155, p. 8, Santa Beatriz, Telf. +511 4728534

Crisógono Francisco **RUBIO**, Experto Sub-Gerencia Planificación Estratégica, Telf. 2101105 crubio@tp.com.pr

Antonio **RODRÍGUEZ**, Asesoría en Telecomunicaciones, Gerencia Central de Regulación y Planificación Estratégica, Telf. 2101109 arodriguezl@tp.com.pe

Gina Valeria **LA ROSA**, Gerencia de Regulación, Av. Jorge Basadre 592, p. 5, Telf. 2104655, gina.larosa@telefonica-data.com.pe

Vanesa Matheus **LUPERDIGA** , Especialista de Ventas, Gerencia de Productos, Av. Jorge Basadre 592, p. 4, of. 401, Torre Azul, San Isidro, Telf. 2224444, vmatheus@tsi.com.pe vanessa.matheus@telefonica-data.com.pe www.telefonica-data.com.pe

José Cabrera **BREA** , Product Manager, Serv. Transaccionales, Gerente de Productos, Av. Jorge Basadre 592, p.4, Of. 404, San Isidro, Telf. 2224444 Ext. 270, jose.cabrera@telefonica-data.com.pe josecabrera@tsi.com.pe www.telefonica-data.com.pe

Ing. Christian A. **VALDIVIA O.**, Gerencia de Regulación Telefónica del Perú S.A., Telf. +51 1 210 1347 Fax: +51 1 419 0532 cvaldivia@tp.com.pe

Sr. Giancarlo **FALCONI**;

Sra. Ursula **BARRIO**;

Sr. Carlos **BARREDA** ;

Sra. Maria Julia **HUISA**;

Ing. Julián **UGARTE**.

Sr. Erick **IRIARTE**, Red Científica Peruana (RCP), Equipo Editorial ALFA-REDI, Lima Telf. Cel. 943 97 29 faia@amauta.rcp.net.pe

VENEZUELA:

Sr. César **OBACH**, Superintendente de Servicios de Certificación Electrónica de Venezuela. cobach@mct.gov.ve

Sr. José B. **DIGIORGIO**, Presidente Cámara Venezolana de Comercio Electrónico (CAVECOM-e), Calle Paseo Colón, edif. Caracas Teleport. Mezzanina, local M3, Maripérez, Caracas 1050, Telf. +58 212 578 3919. info@cavecom-e.org.ve http://www.cavecom-e.org.ve/