Establecimiento de políticas armonizadas en el mercado de las Tecnologías de la Información y la Comunicación en los países ACP

La prueba por medios electrónicos:

Modelos de directrices para políticas y textos legislativos

HIPCAR

Armonización de políticas, legislación y procedimientos reglamentarios de las TIC en el Caribe

Establecimiento de políticas armonizadas en el mercado de las Tecnologías de la Información y la Comunicación en los países ACP

La prueba por medios electrónicos:

Modelos de directrices para políticas y textos legislativos

HIPCAR

Armonización de políticas, legislación y procedimientos reglamentarios de las TIC en el Caribe

Comisión Europea

CARICOM

CTU

ITU

Descargo de responsabilidad

Este documento ha sido elaborado con el apoyo financiero de la Unión Europea. Los puntos de vista expuestos en el mismo no reflejan necesariamente los de la Unión Europea.

Las denominaciones empleadas y la presentación del material, incluidos los mapas, no representan en absoluto opinión alguna de la UIT en relación con la situación jurídica de cualquier país, territorio, ciudad o zona geográfica, o en relación con las fronteras o límites de los mismos. Las menciones a empresas concretas o a ciertos productos no significan que la UIT los recomiende o respalde frente a otros de similar naturaleza que no se mencionan. Este informe no ha pasado por una revisión editorial.

Por favor tenga en cuenta la protección del medio ambiente antes de imprimir este informe.

Prólogo

Las tecnologías de la información y la comunicación (TIC) están configurando el proceso de mundialización. Al reconocer su potencial para acelerar la integración económica de la región del Caribe y acrecentar así su prosperidad y transformación social, el Mercado y la Economía Comunes de la Comunidad del Caribe (CARICOM) ha elaborado una estrategia de TIC centrada en una conectividad y un desarrollo fortalecidos.

La liberalización del sector de las telecomunicaciones es uno de los elementos fundamentales de dicha estrategia. La coordinación de toda la región resulta esencial para que las políticas, legislaciones y prácticas resultantes del proceso de liberalización de cada país no difieran hasta el punto de convertirse en un obstáculo para el desarrollo de un mercado regional.

El proyecto "Mejora de la competitividad en el Caribe mediante la armonización de las políticas, la legislación y los procedimientos reglamentarios de las TIC" (HIPCAR) ha tratado de superar este posible obstáculo reuniendo y acompañando a los 15 países caribeños en el Grupo de Estados de África, el Caribe y el Pacífico (ACP), a medida que formulan y adoptan políticas, legislaciones y marcos reglamentarios de TIC armonizados. Ejecutado por la Unión Internacional de Telecomunicaciones, el proyecto se ha llevado a cabo en estrecha colaboración con la Unión de Telecomunicaciones del Caribe (CTU), que preside el Comité de Dirección de HIPCAR. El Comité de Dirección, compuesto por representantes de la Secretaría de APC y la Dirección General de Desarrollo y Cooperación - EuropeAid (DEVCO, Comisión Europea) se encarga de la ejecución general del proyecto.

Este proyecto se enmarca en el programa de Tecnologías de la Información y la Comunicación de la ACP (@CP-ICT) y está financiado con cargo al 9º Fondo de Desarrollo Europeo (EDF), que es el principal instrumento de ayuda europeo para la cooperación y el desarrollo en los Estados de ACP, y está cofinanciado por la UIT. El proyecto @CP-ICT tiene por objeto ayudar a los gobiernos e institución de ACP a armonizar sus políticas en materia de TIC en el sector mediante la prestación de asesoramiento de alta calidad comparable a escala mundial pero, a su vez, relevante en el ámbito local, así como mediante la formación y la capacitación correspondiente.

Todos los proyectos que reúnen a múltiples partes interesadas se enfrentan al doble desafío de crear una sensación de propiedad compartida y de velar por la obtención de resultados óptimos para todas las partes. HIPCAR ha prestado una atención especial a esta cuestión desde el principio del proyecto en diciembre de 2008. Tras acordarse unas prioridades compartidas, las partes interesadas crearon grupos de trabajo para abordarlas. Después, se definieron las necesidades específicas de la región y, del mismo modo, prácticas regionales con posibilidades de éxito, que posteriormente se compararon a las prácticas y normativas establecidas en otros lugares.

Estas evaluaciones detalladas, que reflejan las peculiaridades propias de los países, sirvieron de base para las políticas y los textos legislativos modelo que ofrecen la perspectiva de un panorama legislativo del que toda la región puede mostrarse orgullosa. Es seguro que el proyecto se convertirá en un ejemplo para otras regiones a la hora de tratar de aprovechar el potencial catalizador de las TIC para acelerar la integración económica y el desarrollo económico y social.

Quisiera aprovechar esta oportunidad para dar las gracias a la Comisión Europea y a la Secretaría de ACP por su contribución financiera. También quisiera dar las gracias a la Secretaría de la Comunidad del Caribe (CARICOM) y la Unión de Telecomunicaciones del Caribe (CTU) por su contribución a estos trabajos. Sin la voluntad política de parte de los países beneficiaros, se habría logrado muy poco. Por ese motivo, deseo manifestar mi más profundo agradecimiento a todos los gobiernos de ACP por su voluntad política que ha permitido que este proyecto sea un rotundo éxito.

Brahima Sanou
Director de la BDT

Agradecimientos

El presente documento es el resultado de las actividades regionales llevadas a cabo en el marco del proyecto de HIPCAR, ''Fortalecimiento de la competitividad en el Caribe mediante la armonización de las políticas, la legislación y los procedimientos reglamentarios de las TIC'', lanzado oficialmente en la isla de Granada en diciembre de 2008.

En respuesta a los retos y las oportunidades que las tecnologías de la información y las comunicaciones (TIC) ofrecen para el desarrollo político, social, económico y medioambiental, la Unión Internacional de Telecomunicaciones (UIT) y la Comisión Europea (CE) han aunado esfuerzos y han firmado un acuerdo con el objetivo de proporcionar "Apoyo para el establecimiento de políticas armonizadas en el mercado de las TIC en los países ACP (África, el Caribe y el Pacífico)'', como parte del Programa ''Tecnologías de la información y las comunicaciones en los países ACP (@CP-ICT)'', en el marco del Noveno Fondo Europeo de Desarrollo (FED), es decir, el proyecto UIT-CE-ACP.

El proyecto global UIT-CE-ACP se ejecuta a través de tres subproyectos adaptados a las necesidades específicas de cada región: el Caribe (HIPCAR), África subsahariana (HIPSSA) y los países Insulares del Pacífico (ICB4PAC)

El Comité de Dirección del HIPCAR, presidido por la Unión de Telecomunicaciones del Caribe (CTU), proporcionó orientación y apoyo a un equipo de consultores, entre ellos el Sr. Gilberto Martíns de Almeida y la Sra. Priscilla Banner. El proyecto del documento fue examinado, debatido y aprobado por amplio consenso por los participantes en dos talleres de consulta del Grupo de Trabajo del HIPCAR sobre la Sociedad de la Información, celebrados respectivamente en Santa Lucía, del 8 al 12 de marzo de 2010, y en Barbados, del 23 al 26 de agosto de 2010 (véanse los anexos). Las notas explicativas sobre el modelo de textos legislativos contenidas en este documento fueron redactadas por el Sr. Martíns de Almeida para abordar, entre otras cosas, las cuestiones planteadas en el segundo taller.

La UIT desea expresar su especial agradecimiento a los delegados de los ministerios caribeños responsables de las TIC, así como de las telecomunicaciones, que participaron en los talleres, así como a los representantes de los Ministerios de justicia y asuntos jurídicos y otros organismos públicos, organismos reguladores, instituciones académicas, la sociedad civil, operadores y organizaciones regionales, por su arduo trabajo y dedicación consagrados a la elaboración del contenido de este informe. Esta participación de amplia base del sector público, en representación de diferentes sectores, permitió que el proyecto pudiera disponer de una gama intersectorial de puntos de vista e intereses. Asimismo, la UIT desea agradecer las contribuciones de la Secretaría de la Comunidad del Caribe (CARICOM) y de la Unión de Telecomunicaciones del Caribe (CTU).

Un documento como éste, que refleja las necesidades y condiciones generales en la región del Caribe, así como las mejores prácticas a nivel internacional, no habría podido elaborarse sin la participación activa de todas esas partes interesadas.

Las actividades han sido realizadas por la Sra. Kerstin Ludwig, encargada de la coordinación de las actividades en el Caribe (Coordinadora de Proyectos de HIPCAR), y el Sr. Sandro Bazzanella, encargado de la gestión de todo el proyecto que abarca el África Subsahariana, el Caribe y el Pacífico (Director de Proyecto UIT-CE-ACP) con el apoyo global de la Sra. Nicole Morain, Asistente de Proyecto de HIPCAR, y de la Sra. Silvia Villar, Asistente de Proyecto UIT-CE-ACP. La labor se llevó a cabo bajo la dirección general del Sr. Cosmas Zavazava, Jefe del Departamento de Apoyo a los Proyectos y Gestión del Conocimiento (PKM). El documento también se benefició de los comentarios de la División de Aplicaciones de las TIC y Ciberseguridad (CYB) de la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT. El Sr. Philip Cross, Representante de Zona de la UIT para el Caribe, también prestó su apoyo. El equipo del Servicio de Composición de Documentos de la UIT se encargó de su publicación.

Índice

Página

Introducción

1.1. Proyecto HIPCAR – Objetivos y beneficiarios

La Unión Internacional de Telecomunicaciones (UIT) y la Comisión Europea (CE), en estrecha colaboración con la Secretaría de la Comunidad del Caribe (CARICOM) y la Unión de Telecomunicaciones del Caribe (CTU), presentaron oficialmente el proyecto HIPCAR[1] en diciembre de 2008 en el Caribe. El proyecto HIPCAR forma parte de un proyecto global UIT-CE-ACP, que también abarca a los países del África subsahariana y el Pacífico.

El objetivo del HIPCAR es prestar ayuda a los países CARICOM/ACP/CARIFORUM[2] en el Caribe para armonizar sus políticas, legislación y procedimientos reglamentarios relativos a las tecnologías de la información y las comunicaciones (TIC) con el fin de facilitar la integración del mercado, impulsar las inversiones en mejores capacidades y servicios de las TIC, y ampliar la protección de los intereses de los consumidores en toda la región. En definitiva, el objetivo del proyecto es mejorar, mediante las TIC, la competitividad y el desarrollo socioeconómico y cultural en la región del Caribe.

De conformidad con el Artículo 67 del Tratado de Chaguaramas revisado, el HIPCAR puede considerarse parte integrante de los esfuerzos de la región para el desarrollo de un mercado y economía únicos de la Comunidad del Caribe (CARICOM) a través de la liberalización progresiva del sector de servicios de las TIC. El proyecto también brinda su apoyo al programa de conectividad para la CARICOM y los compromisos asumidos respecto de la región en la Cumbre Mundial de la Sociedad de la Información (CMSI), al Acuerdo General sobre el Comercio de Servicios, de la Organización Mundial del Comercio (AGCS-OMC) y los Objetivos de Desarrollo del Milenio (ODM). Asimismo, apunta directamente a promover la competitividad y un mejor acceso a los servicios, en el contexto de los compromisos contraídos en diversos tratados, como por ejemplo el Acuerdo de Asociación Económica de los Estados del CARIFORUM con la Unión Europea (UE-CARIFORUM)

Los países beneficiarios del proyecto HIPCAR son Antigua y Barbuda, las Bahamas, Barbados, Belice, Dominica, la República Dominicana, Granada, Guyana, Haití, Jamaica, Saint Kitts y Nevis, Santa Lucía, San Vicente y las Granadinas, Suriname, y Trinidad y Tobago.

1.2. Comité de Dirección del proyecto y Grupos de Trabajo

El proyecto HIPCAR ha establecido un Comité de Dirección encargado de proporcionar la necesaria orientación y supervisión. El Comité está integrado por representantes de la Secretaría de la Comunidad del Caribe (CARICOM), la Unión Internacional de Telecomunicaciones del Caribe (CTU), la Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL), la Asociación de Organizaciones Nacionales de Telecomunicaciones del Caribe (CANTO), la Comunidad Virtual de las TIC del Caribe (CIVIC) y la Unión Internacional de Telecomunicaciones (UIT).

---

1 El nombre completo del proyecto HIPCAR es ''Mejorar la competitividad en el Caribe a través de la armonización de las políticas, la legislación y los procedimientos reglamentarios relativos a las TIC''. HIPCAR forma parte de un proyecto global UIT-CE-ACP que se lleva a cabo con una financiación de la Unión Europea fijada en 8 millones de euros y un complemento de 500 000 USD aportados por la Unión Internacional de Telecomunicaciones (UIT). La ejecución está a cargo de la UIT, en colaboración con la Unión de Telecomunicaciones del Caribe (CTU) y con la participación de otras organizaciones de la región.
(véase www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

2 El CARIFORUM es una organización regional de 15 países independientes en la región del Caribe (Antigua y Barbuda, las Bahamas, Barbados, Belice, Dominica, la República Dominicana, Granada, Guyana, Haití, Jamaica, St. Kitts y Nevis, Santa Lucía, San Vicente y las Granadinas, Suriname, y Trinidad y Tobago). Todos estos Estados son signatarios de los Convenios ACP-CE.

Con el fin de garantizar la contribución de los interesados y pertinencia para cada país, se establecieron también los Grupos de Trabajo HIPCAR, cuyos integrantes fueron designados por los gobiernos de los países, y abarcaban especialistas de los organismos de TIC, representantes de organismos judiciales y de otras instituciones públicas, órganos nacionales de regulación, centros nacionales de coordinación de las TIC y personas responsables de la elaboración de la legislación nacional. Los Grupos de Trabajo también incluyen a representantes de organismos regionales relevantes (Secretaría de la CARICOM, CTU, ECTEL y CANTO) y observadores de otras entidades regionales interesadas (por ejemplo, la sociedad civil, el sector privado, los operadores, las instituciones académicas, etc.).

Los Grupos de Trabajo se han encargado de los dos ámbitos de trabajo siguientes:

1. *Políticas y marco legislativo de las TIC en relación con los temas de la sociedad de la información,* que abarca seis subtemas: comercio electrónico (transacciones y prueba), privacidad y protección de datos, interceptación legal de comunicaciones, ciberdelincuencia y acceso a la información pública (libertad de información).
2. *Políticas y marco legislativo de las TIC en relación con las telecomunicaciones,* que abarca tres subtemas: acceso/servicio universal, interconexión y concesión de licencias en un entorno convergente.

Los informes de los Grupos de Trabajo publicados en esta serie de documentos se estructuran en torno a estos dos ámbitos de trabajo principales.

1.3. Contenido y ejecución del proyecto

Las actividades del proyecto se iniciaron con una mesa redonda de presentación del proyecto, organizada en la isla de Granada los días 15 y 16 de diciembre de 2008. Hasta la fecha, todos los países beneficiarios del HIPCAR (con excepción de Haití) han participado activamente en las reuniones del HIPCAR, junto con las organizaciones asociadas al proyecto, reguladores, operadores, instituciones académicas y la sociedad civil que, además del evento de presentación del proyecto en Granada, incluyen talleres regionales en Trinidad y Tobago, St. Lucia, Saint Kitts y Nevis, Suriname y Barbados.

Las actividades principales del proyecto han estado dirigidas por equipos de expertos regionales e internacionales que han colaborado con los miembros de los Grupos de trabajo, con un enfoque centrado en los ámbitos antes mencionados.

Durante la *Fase I* (ya finalizada), el proyecto HIPCAR:

1. ha analizado las legislaciones existentes en los países beneficiarios para compararlas con las mejores prácticas a nivel internacional, y en el contexto de la armonización en la región; y
2. ha diseñado un modelo de directrices para políticas y un modelo de textos legislativos en los ámbitos señalados, como punto de partida para formular políticas nacionales y una legislación o reglamentaciones nacionales sobre las TIC.

Se pretende que estas propuestas sean validadas o respaldadas por la CARICOM/CTU y por las autoridades de los países de la región, como base para la siguiente fase del proyecto.

los modelos indicados en políticas y legislaciones nacionales sobre las TIC, adaptadas a sus necesidades, circunstancias y prioridades específicas. Con miras a la consecución de este objetivo, el HIPCAR dispone de fondos para responder a las peticiones de asistencia técnica de dichos países, incluso para la creación de capacidad.

1.4. Reseña general de los seis modelos de directrices para políticas y textos legislativos del HIPCAR que abordan cuestiones de la sociedad de la información

Todos los países del mundo, entre ellos los del Caribe, buscan formas de establecer marcos jurídicos para abordar las necesidades de la sociedad de la información, con miras a aprovechar la creciente ubicuidad de Internet como canal de prestación de servicios, y garantizar un entorno seguro y una capacidad de tratamiento de datos de los sistemas de información que contribuya a mejorar la eficiencia y eficacia de las actividades.

La sociedad de la información se basa en la premisa del acceso a la información y los servicios, así como la utilización de sistemas automatizados de tratamiento de la información que mejoren la prestación de servicios a los mercados y las personas en cualquier parte del mundo. La sociedad de la información en general, y el acceso a las tecnologías de la información y las comunicaciones (TIC) en particular, ofrecen oportunidades únicas, tanto a los usuarios particulares como a las empresas. Dado que los imperativos básicos del comercio no han cambiado, la transmisión inmediata de información comercial genera oportunidades para mejorar las relaciones de negocios. Esta facilidad de intercambio de información comercial introduce nuevos paradigmas: en primer lugar, cada vez que se utiliza la información para apoyar las transacciones relacionadas con bienes físicos y servicios tradicionales, y en segundo lugar, cuando esa propia información es el producto principal objeto de transacción.

La disponibilidad de las TIC y de nuevos servicios basados en redes ofrece una serie de ventajas para la sociedad en general, y especialmente para los países en desarrollo. Algunas aplicaciones de las TIC, que introducen los medios electrónicos en ámbitos como la administración, el comercio, la educación, la salud y el medio ambiente, se consideran factores propicios del desarrollo, ya que ofrecen un canal eficiente para prestar una amplia gama de servicios básicos en zonas rurales y distantes. Esas aplicaciones de las TIC pueden facilitar el logro de los Objetivos de Desarrollo del Milenio, reducir la pobreza y mejorar el estado de la salud y el medio ambiente en los países en desarrollo. El libre acceso a la información puede además servir de sustento a los procesos democráticos, ya que el flujo de información escapa al control de las autoridades estatales (como ha sucedido, por ejemplo, en Europa oriental). Si se dan el enfoque, el contexto y los procesos de ejecución adecuados, las inversiones en aplicaciones y herramientas de las TIC pueden contribuir a mejorar considerablemente la productividad y la calidad.

Sin embargo, este proceso de transformación también presenta problemas, en la medida en que el marco jurídico actual no atiende necesariamente a las necesidades específicas que surgen en un entorno tecnológico en constante evolución. Cuando la información se usa para apoyar el comercio de bienes y servicios tradicionales, es preciso clarificar de qué manera afecta a los supuestos comerciales tradicionales; y cuando la información es el propio producto objeto de comercio, es necesario proteger al creador o propietario de ese producto. En ambos casos, se debe justificar cómo se detectan, se persiguen y se suprimen las conductas indebidas, teniendo en cuenta que en realidad se trata de transacciones transfronterizas, basadas en productos intangibles.

Los seis modelos de marcos interrelacionados

El HIPCAR ha elaborado seis modelos interrelacionados que sientan un marco jurídico exhaustivo para abordar la evolución constante del entorno de las sociedades de la información, al ofrecer orientación y apoyo para establecer una legislación armonizada en los países beneficiarios del proyecto.

En primer lugar, se ha elaborado un marco jurídico para proteger el derecho de los usuarios en un entorno en evolución y, de este modo, granjearse, entre otros aspectos, la confianza de consumidores e inversores en la certidumbre jurídica y la protección de la privacidad. Se han preparado modelos de textos legislativos del HIPCAR que abordan aspectos relacionados con los ámbitos de **Acceso a la información pública (libertad de información)**, con miras a fomentar una cultura adecuada de transparencia en las cuestiones de reglamentación, en provecho de todos los interesados; y **Privacidad y protección de datos**, con miras a garantizar la intimidad y la protección de la información personal de los particulares. Este último marco se centra en las prácticas de confidencialidad adecuadas, en los sectores público y privado.

En segundo lugar, se ha elaborado otro modelo de texto legislativo sobre las **Transacciones en el comercio electrónico**, que incluye la firma electrónica, con el objeto de facilitar la armonización de las leyes en lo que respecta a la validez jurídica de las prácticas de formación de los contratos y las previsiones en caso de incumplimiento. Este marco se orienta a equiparar los documentos y contratos impresos y los electrónicos, así como a sentar las bases para el comercio en el ciberespacio. El marco para las transacciones en el comercio electrónico está acompañado de un texto legislativo relativo a la **prueba por medios electrónicos**, destinado a reglamentar los medios de prueba jurídicos en los procedimientos civiles y penales.

Para garantizar que los órganos de cumplimiento de la ley puedan investigar las violaciones graves al carácter confidencial, integridad y disponibilidad de las TIC y de los datos, se prepararon modelos de textos legislativos para armonizar la legislación en materia penal y de procedimiento penal. El texto legislativo sobre la **ciberdelincuencia** define los delitos, los instrumentos de investigación y la responsabilidad penal de los principales agentes. Otro texto legislativo trata sobre la **interceptación de comunicaciones electrónicas** y establece un marco apropiado que prohíbe interceptar de forma ilegal esas comunicaciones, y define un estrecho margen de situaciones en que los órganos encargados de hacer cumplir la ley pueden hacerlo, siempre que se den determinadas condiciones claramente definidas.

Elaboración de los modelos de textos legislativos

Los modelos de textos legislativos se elaboraron teniendo en cuenta los principales elementos de las tendencias internacionales, así como las tradiciones jurídicas y las mejores prácticas de la región. El proceso se inició para obtener marcos jurídicos que puedan satisfacer de forma óptima las realidades y necesidades de los países beneficiarios del HIPCAR en la región, para los cuales y por los cuales se establecieron esos modelos. Por consiguiente, el proceso supuso una importante interacción con partes interesadas en cada etapa de su elaboración.

El primer paso en este complejo proceso fue evaluar los marcos legales existentes en la región, mediante un examen de las leyes relativas a todos los ámbitos pertinentes. Además de la legislación en vigor, también se examinaron, cuando se consideró oportuno, los proyectos de ley ya preparados, pero todavía en proceso de promulgación. En un segundo paso, se identificaron las mejores prácticas internacionales (por ejemplo de las Naciones Unidas, la OCDE, la Unión Europea, el Commonwealth, la CNUDMI y la CARICOM), así como las legislaciones nacionales más avanzadas (por ejemplo, del Reino Unido, Australia, Malta y el Brasil, entre otras). Estas prácticas se utilizaron como base de referencia.

Se procedió a complejos análisis jurídicos en cada uno de los seis ámbitos, a los fines de comparar la legislación vigente en la región con la base de referencia mencionada. Este análisis de derecho comparado produjo una imagen del nivel de adelanto en los principales ámbitos de política dentro de la región. Las conclusiones fueron instructivas y mostraron que los marcos relativos a las transacciones electrónicas, la ciberdelincuencia (o ''utilización abusiva de la informática'') y el acceso a la información pública (libertad de información) estaban más avanzados que los de los demás temas.

Sobre la base de los resultados de este análisis comparado de las legislaciones, los agentes regionales establecieron los componentes básicos de políticas de referencia que, una vez aprobadas por las partes interesadas, sentaron los fundamentos para continuar la deliberación sobre política y la elaboración de los textos legislativos. Dichos componentes básicos confirmaron algunas tendencias y temas comunes encontrados en la jurisprudencia internacional, pero a la vez sirvieron para definir algunas consideraciones particulares que deberían incluirse, en el contexto de una región formada por un conjunto de pequeños Estados insulares soberanos en desarrollo. Por ejemplo, una de las principales consideraciones específicas que afectó a las deliberaciones, en esta y otras etapas del proceso, fue la cuestión de la capacidad institucional para asumir una administración adecuada de estos nuevos sistemas.

Los componentes básicos se utilizaron a continuación para elaborar modelos de textos legislativos adaptados, que se ajustaran al mismo tiempo a las normas internacionales y a las necesidades de los países beneficiarios del HIPCAR. Seguidamente, los interesados evaluaron nuevamente cada modelo de

texto, desde el punto de vista de la viabilidad y su aplicabilidad inmediata a diferentes contextos regionales. Este grupo de interesados – formado por legisladores y expertos en política de la región – preparó textos que reflejaban de la mejor manera posible la convergencia de las normas internacionales con las consideraciones locales. La amplia participación de representantes de casi todos los 15 países beneficiarios del HIPCAR, entre ellos reguladores, operadores, organizaciones regionales, la sociedad civil e instituciones académicas, garantizó la compatibilidad de los textos legislativos con las diferentes normas jurídicas de la región. No obstante, también se contempló la posibilidad de que cada Estado beneficiario pudiera tener sus preferencias particulares con respecto a la aplicación de determinadas disposiciones. Por tanto, los modelos de textos también ofrecen diferentes opciones dentro del carácter general de un marco armonizado. Tal enfoque apunta a facilitar la aceptación generalizada de los documentos y aumentar la posibilidad de aplicarlos oportunamente en las jurisdicciones de todos los países beneficiarios.

Interacción y superposición de la cobertura de los modelos de textos

Por la propia índole de las cuestiones objeto de examen, hay elementos comunes que se recogen en los seis marcos.

En primer lugar, se deben considerar los marcos que contemplan el uso de medios electrónicos en la comunicación y en la actividad comercial, en cuestiones como **las transacciones en el comercio electrónico**, **la prueba por medios electrónicos**, **la ciberdelincuencia** y **la interceptación de las comunicaciones.** Los cuatro marcos abordan aspectos relacionados con el tratamiento de los mensajes transmitidos a través de redes de comunicaciones, el establecimiento de pruebas apropiadas para determinar la validez de los registros o documentos, y la incorporación generalizada de sistemas orientados a tratar de forma equivalente los documentos impresos y electrónicos en los procesos de protección contra comportamientos indebidos, la atención al consumidor y los procedimientos de solución de controversias.

En este sentido, entre todos estos marcos hay varias definiciones comunes que se deben tener en cuenta, cuando se considere necesario, para evaluar los diversos alcances de su aplicabilidad. Algunos conceptos comunes son: ''red de comunicaciones electrónicas'' – que se debe alinear con la definición de las leyes de telecomunicaciones vigentes de la jurisdicción; ''documento electrónico'' o ''registro electrónico'' – que deben reflejar una interpretación amplia, a fin de incluir el material sonoro y de vídeo; y ''firma electrónica'', ''firma electrónica avanzada'', ''certificados'', ''certificados de acreditación'', ''proveedores de servicios de certificación'' y ''autoridades de certificación'', conceptos todos que se relacionan con la aplicación de técnicas de cifrado para validar de forma electrónica la autenticidad y con el reconocimiento del sector tecnológico y económico que se ha desarrollado alrededor de la prestación de esos servicios.

En este contexto, el marco dedicado a las **transacciones en el comercio electrónico** establece, entre otras cosas, los principios básicos de reconocimiento y atribución necesarios para la eficacia de los otros marcos. Se centra en definir los principios fundamentales que se han de emplear para determinar si los casos son de naturaleza civil o mercantil. Este marco también es esencial para definir una estructura de mercado adecuada y una estrategia realista para la supervisión del sector, en aras del interés del público y la confianza del consumidor. Las decisiones que se adopten en las cuestiones relativas a este sistema administrativo tendrán un efecto ulterior en la forma de utilizar la firma electrónica con fines de prueba en el procedimiento, y la manera de atribuir adecuadamente las responsabilidades y obligaciones definidas en la ley.

Esa presunción de equivalencia permite que los otros marcos puedan abordar adecuadamente los aspectos básicos relacionados con el tratamiento adecuado de las transferencias de información por medios electrónicos. El marco de la **ciberdelincuencia**, por ejemplo, define los delitos relacionados con la interceptación y la alteración de la comunicación, así como el fraude informático. El marco sobre **la prueba en el comercio electrónico** sienta las bases para presentar la prueba por medios electrónicos como una nueva categoría de prueba.

Un importante elemento común de **las transacciones electrónicas** y **la ciberdelincuencia** es la determinación de las responsabilidades y compromisos que asumen los proveedores de servicios cuando dichos servicios se utilizan para un proceder malintencionado con empleo de medios electrónicos. Se ha prestado especial atención a obrar con coherencia a la hora de determinar las partes destinatarias de las secciones pertinentes y atribuir adecuadamente las obligaciones y su cumplimiento.

En el caso de los marcos orientados a mejorar la supervisión reglamentaria y la confianza del usuario, los modelos de textos elaborados por el HIPCAR tratan con los extremos opuestos de una misma cuestión: mientras que el modelo dedicado al **Acceso a la información pública** procura promover la divulgación de la información pública, con excepciones concretas, el modelo de P**rivacidad y protección de datos** fomenta la protección de un subconjunto de información que se considera no abarcado por el modelo anterior. Es importante destacar que estos dos marcos se orientan a fomentar la mejora en la gestión de documentos y las prácticas de mantenimiento de registros dentro del sector público y, en el caso del último marco, también algunos aspectos del sector privado. Sin embargo, es de destacar que, a diferencia de los otros cuatro modelos de textos, estos marcos no se aplican exclusivamente a los medios electrónicos ni pretenden crear un marco en el que las consideraciones sobre un nuevo medio se superpongan a los procedimientos existentes. Para garantizar la coherencia en este sentido, los marcos se orientan a regular la gestión adecuada de los recursos de información, tanto en formato electrónico como no electrónico.

Entre estos dos marcos legislativos existen algunos factores de superposición estructural y logística, entre ellos, la definición de conceptos clave como ''autoridad pública'' (personas a quienes se aplicarían los marcos), ''información'', ''datos'' y ''documento'', así como su relación mutua. Otra forma importante de superposición se refiere a la supervisión adecuada de estos marcos. Ambos requieren el establecimiento de órganos de supervisión suficientemente independientes de influencias externas, para garantizar al público la ecuanimidad de sus decisiones. Estos organismos independientes también deberían tener la capacidad de imponer multas y/o sanciones contra las partes que ejecuten actividades dirigidas a frustrar los objetivos de alguno de estos marcos.

Conclusión

Los seis modelos de textos legislativos del HIPCAR ofrecen a los países beneficiarios del proyecto un marco global para abordar la mayoría de aspectos pertinentes sobre la reglamentación de las cuestiones relativas a la sociedad de la información. En su redacción se reflejan tanto las normas internacionales más actuales como las necesidades de los pequeños Estados insulares en desarrollo del Caribe en general y, más específicamente, de los países beneficiarios del proyecto HIPCAR. La amplia participación de las partes interesadas de los países beneficiarios en todas las fases de elaboración de los modelos de textos legislativos garantiza que este modelo se apruebe de manera fácil y oportuna. Aunque el enfoque se ha centrado en las necesidades de los países de la región del Caribe, algunos países de otras regiones del mundo ya han determinado que esos modelos de textos legislativos también pueden servir como posibles directrices.

Dada la índole específica e interrelacionada de los modelos de textos del HIPCAR, para los países beneficiarios del proyecto será más ventajoso elaborar e introducir una legislación basada en esos modelos de forma coordinada. Por ejemplo, los modelos relativos al comercio electrónico (transacciones y prueba) funcionarán más eficazmente si los marcos sobre ciberdelincuencia e interceptación de las comunicaciones se elaboran y aprueban simultáneamente, ya que están estrechamente relacionados y son interdependientes para abordar los problemas relacionados con un desarrollo reglamentario sólido. Del mismo modo, los marcos sobre acceso a la información pública y la privacidad y protección de datos contienen esas sinergias en lo que se refiere al entorno administrativo y los requisitos en materia de aptitudes básicas, por lo que su aprobación simultánea necesariamente ha de reforzar ambos marcos en el momento de su aplicación.

De este modo, se creará una oportunidad óptima de utilizar el marco establecido para la región de forma integral.

1.5. El presente informe

Este informe se refiere a la prueba por medios electrónicos en el comercio electrónico, uno de los ámbitos abordados por el Grupo de Trabajo sobre políticas y marco legislativo de las TIC en relación con los temas de la sociedad de la información. Incluye un modelo de directrices para políticas y un modelo de texto legislativo con notas explicativas que los países del Caribe tal vez deseen utilizar para la formulación o actualización de sus propias políticas y legislaciones nacionales en esta materia.

Antes de redactar este documento, el equipo de expertos del HIPCAR, en estrecha colaboración con los miembros del mencionado grupo de trabajo, preparó y revisó una evaluación de la legislación vigente sobre cuestiones de la sociedad de la información en los 15 países beneficiarios del Proyecto. La evaluación se centró en seis ámbitos: transacciones en el comercio electrónico, prueba por medios electrónicos en el comercio electrónico, privacidad y protección de datos, interceptación de las comunicaciones, ciberdelincuencia y acceso a la información pública (libertad de información). Esta evaluación tuvo en cuenta las mejores prácticas a nivel internacional y regional.

Esta evaluación regional, publicada por separado como un documento complementario al informe actual[3], abarcaba un análisis comparado de la legislación vigente sobre la prueba por medios electrónicos en el comercio electrónico en los países beneficiarios del HIPCAR, y la identificación de las posibles deficiencias en este sentido, como base para preparar los modelos de directrices para políticas y de textos legislativos que se presentan. Al recoger las mejores prácticas y normas nacionales, regionales e internacionales[4], velando siempre por la compatibilidad con las tradiciones jurídicas en el Caribe, los modelos de documentos contenidos en este informe están orientados a satisfacer y responder a las necesidades específicas de la región.

El Comité de Dirección del HIPCAR, presidido por la Unión de Telecomunicaciones del Caribe (CTU), prestó orientación y apoyo a un equipo de consultores, entre ellos el Sr. Gilberto Martíns de Almeida y la Sra. Priscilla Banner. El modelo de texto jurídico sobre la prueba por medios electrónicos en el comercio electrónico se elaboró en tres fases: 1) redacción de un informe de evaluación, 2) preparación del modelo de directrices para políticas; y 3) redacción de un modelo de texto legislativo. Posteriormente, los participantes en dos talleres de consulta del Grupo de Trabajo del HIPCAR sobre la sociedad de la información, celebrados en Santa Lucía del 8 al 12 de marzo de 2010, y en Barbados del 23 al 26 de agosto de 2010, examinaron, debatieron y aprobaron por amplio consenso el proyecto del documento (véanse los anexos). Las notas explicativas sobre el modelo de texto legislativo contenidas en este documento fueron redactadas por el Sr. Martíns de Almeida con el objetivo de abordar, entre otras cosas, las cuestiones planteadas en el segundo taller. El Comité de Dirección del proyecto HIPCAR y el equipo de gestión del proyecto supervisaron el proceso de elaboración de estos documentos. Este documento contiene por lo tanto los datos e información conocidos en agosto de 2010.

Después de este proceso, los documentos se ultimaron y distribuyeron a todos los interesados, para su consideración por los Gobiernos de los países beneficiarios del HIPCAR.

---

3 Véase *ICT Policy and Legislative Framework on Information Society Issues – Electronic Evidence in e-Commerce: Assessment Report on the Current Situation in the Caribbean*, disponible en www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/.

4 Tal como se refleja en: *Toolkit for Cybercrime Legislation and Understanding Cybercrime: A Guide for Developing Countries* ; la Ley Modelo del Commonwealth sobre la prueba por medios electrónicos (LMM(02)1), la Directiva 2002/58/EC; y los enfoques de los países, tanto dentro como fuera de la región.

1.6. La importancia de una política y legislación eficaces sobre la prueba por medios electrónicos en el comercio electrónico

El comercio electrónico, así como otras aplicaciones de las TIC en la actualidad, se basa en la admisibilidad legal de la prueba por medios electrónicos como condición fundamental para generar la confianza necesaria para la expansión de dicho comercio. Así lo ha reconocido la comunidad internacional, como se pone de manifiesto en las leyes modelo sobre la prueba por medios electrónicos de la CNUDMI y del Commonwealth, así como en la legislación pertinente sobre la materia aplicada en un gran número de Estados.

Es un hecho que los crecientes peligros para la integridad, disponibilidad, confidencialidad, autenticidad y autoría de los documentos electrónicos resultantes de las acciones de las distintas formas de piratería informática, como los *hackers*, *crackers* y *re-mailers* (reenviadores de correos electrónicos), así como los fraudes empresariales y los delitos cibernéticos en general, han causado una gran preocupación con respecto a los riesgos y limitaciones que supone la admisibilidad judicial de las pruebas por medios electrónicos.

Por otro lado, la proliferación de normas y marcos internacionales sobre la seguridad de la información y la gestión de las TI, las firmas digitales de alta seguridad, las técnicas de indicación de tiempo y los procedimientos jurídicos electrónicos han generado la convicción generalizada de que las pruebas por medios electrónicos pueden ser tan seguras y fiables, o incluso más, que las convencionales (no electrónicas), siempre que se tomen ciertas precauciones.

Teniendo en cuenta las tendencias y posibilidades contrapuestas en este campo, es preciso crear un equilibrio mediante una reglamentación que concilie los aspectos técnicos y los de procedimiento a fin de obtener pruebas a un coste razonable y respetar principios bien aceptados como el principio de equivalencia entre la prueba digital y la no digital, el principio de precaución (que requiere de la adopción de medidas de prevención o de reducción de riesgos) y el principio de acreditación (que exige la certificación acreditada de los procedimientos, para inspirar un mayor nivel de confianza).

La reglamentación de la prueba digital plantea varias dificultades, como la protección equilibrada del derecho a la privacidad y a no declarar contra sí mismo. La retención de datos y el cifrado son ejemplos en que la presentación de pruebas digitales se sitúa en el cruce entre los intereses de la seguridad y de la privacidad.

La falta de una regulación local sobre la prueba digital es un hecho bien ponderado por los *hackers* y otros ciberdelincuentes, que dirigen sus ataques contra países menos preparados para utilizar las pruebas por medios electrónicos en la persecución de los delitos. Los sistemas *botnet* (conjunto de robots informáticos automatizados) son un ejemplo de las amenazas que se plantean a los ciudadanos, gobiernos y empresas de los países que no tienen una legislación específica sobre directrices y criterios aplicables a la admisibilidad de la búsqueda, generación, obtención y conservación de pruebas digitales.

El impulso de los Estados para introducir una legislación sobre la prueba por medios electrónicos, o modificar la existente sobre pruebas, a fin de incluir las de naturaleza electrónica, se basa en el reconocimiento de que las normas tradicionales sobre pruebas basadas en el *common law* que se utilizan para hacer cumplir los derechos civiles y penales en este campo, no son suficientes para recoger los avances tecnológicos, y por lo tanto necesitan ser modernizadas. La naturaleza de la propia prueba por medios electrónicos (su carácter novedoso y el hecho de que puede ser percibida como frágil y fácilmente manipulable) plantea problemas a los países en el proceso de actualización de sus leyes. Por su fragilidad, esa prueba podría ser alterada, dañada o destruida por una manipulación o examen inadecuados. Además, esa prueba tiene a menudo un carácter transnacional, por ejemplo, cuando los servidores están ubicados en varios países, lo que aumenta la dificultad para utilizarla y para que un tribunal de justicia la admita debidamente.

Introducción

En 2002, la Secretaría del Commonwealth recomendó a los países que lo integran que adoptaran o adaptaran su modelo de legislación en este ámbito. Desde entonces, el rápido ritmo del progreso tecnológico y la creciente sofisticación y expansión de la delincuencia informática han planteado nuevos retos a los países interesados en reglamentar la prueba por medios electrónicos. En este sentido, como otros ejemplos de nuevos temas que se deben considerar figuran la informática en ''la nube de Internet'', la criptografía, el servicio de indicación de tiempo, los procedimientos jurídicos electrónicos y las nuevas normas internacionales.

En este contexto, la reglamentación sobre la prueba por medios electrónicos debe articularse de forma conjunta con la reglamentación en ámbitos como los procedimientos expeditivos para la conservación de los datos, la orden de presentación, allanamiento e incautación, la retención de los datos, y otros, con el fin de velar por su eficacia.

Sección I:
Modelo de directrices para políticas – La prueba por medios electrónicos

A continuación se presenta el modelo de directrices para políticas que un país puede considerar en relación con la prueba por medios electrónicos en el comercio electrónico.

1. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM SE PONDRÁN COMO OBJETIVO ESTABLECER LAS INTERPRETACIONES COMUNES NECESARIAS PARA LOS TÉRMINOS CLAVE RELACIONADOS CON LA PRUEBA POR MEDIOS ELECTRÓNICOS[5]

- Habrá una definición adecuada de ''ordenador/computador'', ''dispositivo'', ''datos del ordenador/computador'', ''sistema informático'', ''datos sobre contenido'', ''datos sobre tráfico'', ''datos sobre ubicación'', ''documento'', ''registro electrónico'', ''documento electrónico'', ''firma electrónica'', ''firma digital'' e ''indicación de tiempo''.
- La formulación de la definición de estos términos será lo suficientemente amplia, e irá acompañada de una lista de ejemplos ilustrativos.
- Se determinará la terminología que se utilizará a los fines de la interpretación judicial dentro de la jurisdicción de cada Estado beneficiario, y la manera de seguir de cerca esa actividad judicial para mantener una armonía entre las definiciones legales y las judiciales.

2. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM SE PONDRÁN COMO OBJETIVO ESTABLECER EL MARCO NECESARIO PARA DEFINIR EL ORIGEN PÚBLICO O PRIVADO Y LAS FUNCIONES DE LAS PARTES ENCARGADAS DE RECOPILAR Y/O GESTIONAR LA PRUEBA ELECTRÓNICA[6]

- La Ley contendrá disposiciones que establezcan el papel de las ''autoridades públicas'', la fiscalía y la policía en la recopilación y/o gestión de pruebas por medios electrónicos y, en su caso, de las ''autoridades de certificación'', ''proveedores de servicios de certificación'', ''registradores'' y ''acceso sin interrupción''.
- Se dispondrá que las autoridades públicas se ajusten a las normas para la recopilación y gestión de pruebas por medios electrónicos contenidas en las leyes o políticas sobre seguridad de la información pública (por ejemplo, respecto a los límites en el uso de la criptografía, los procedimientos en el uso de dispositivos, y otros protocolos compatibles con las mejores prácticas internacionales en investigación forense digital).
- Se establecerán disposiciones que reconozcan la regulación conjunta o autorregulación de algunos sectores de mercado o de actividades, especialmente cuando la firma digital y el uso de otras tecnologías no ofrezca una relación razonable coste/beneficio.
- Se establecerán disposiciones que fijen los principios y ámbitos en que la admisibilidad de la prueba por medios electrónicos se basará principalmente en las normas de procedimiento.
- Se establecerán disposiciones que fijen y apliquen las normas técnicas destinadas a fomentar la adecuada recopilación y gestión de pruebas por medios electrónicos.

…/…

[5] Debería lanzarse una campaña a fin de sensibilizar a la población sobre la importancia de la prueba por medios electrónicos, que incluya una explicación de los términos clave, según el criterio de cada Estado beneficiario.

[6] Se deberá aplicar una política pública de formación de aptitudes en el Poder Judicial, para que los jueces y expertos técnicos se familiaricen con el uso de los conceptos clave relativos a la prueba por medios electrónicos, la terminología y las normas de procedimiento. Igualmente, se deberá aplicar una política pública dirigida a fomentar la cooperación institucional para la creación de aplicaciones que utilicen la prueba por medios electrónicos como medio para lograr una mayor automatización de los servicios públicos mediante el uso de la electrónica.

- Cuando proceda, se incluirán disposiciones que establezcan el principio de reciprocidad para el reconocimiento o no de los certificados digitales emitidos en un tercer país, en virtud de la autoridad y las leyes regionales comunes;
- Cuando proceda, se incluirán disposiciones que establezcan que la autoridad pública se extenderá, en algunos casos, a las entidades privadas, siempre que estas entidades estén autorizadas para actuar como ''notarios electrónicos'', es decir, terceros que proporcionen a las partes la autenticación digital sin necesidad de ajustarse a las pruebas técnicas y de procedimiento de los proveedores de servicios de certificación registrados.
- Cuando proceda, se definirán los elementos de esta opción de ''notarización'' y, por lo tanto, el alcance de las funciones de un notario electrónico en cuanto a los derechos y deberes asociados desde el punto de vista jurídico.

3. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM DEFINIRÁN LOS MANDATOS JURÍDICOS Y LAS NORMAS A QUE DEBE SOMETERSE LA PRUEBA POR MEDIOS ELECTRÓNICOS

- La ley o el mandato jurídico definirá el ''sistema de registros electrónicos'' a los efectos de la interpretación de esta política.
- La ley o el mandato jurídico deberá tener un objetivo habilitador y no contener disposiciones demasiado prescriptivas.
- La ley o el mandato jurídico dispondrá que no se privará de efecto jurídico a un documento por el solo hecho de ser electrónico.
- Cuando proceda, la ley o el mandato jurídico determinará en qué medida las normas de procedimiento relativas a la recopilación, gestión y/o uso de registros electrónicos sustentarán la admisibilidad de los documentos electrónicos y en qué circunstancias se requerirá la presentación de pruebas electrónicas de carácter técnico.
- La ley o el mandato jurídico especificará los fundamentos jurídicos de la prueba por medios electrónicos, y ampliará claramente su admisibilidad en las actuaciones administrativas y judiciales (en materia civil, mercantil, penal, laboral, administrativa y de otro tipo).
- La ley o el mandato jurídico establecerá la naturaleza y los efectos de la presunción legal asociada a la prueba por medios electrónicos, a fin de que se la pondere en relación con otros tipos de prueba (documental, etc.).
- La ley o el mandato jurídico definirá y dispondrá la publicación de información sobre las normas adecuadas para la actualización, almacenamiento y eliminación de pruebas por medios electrónicos.
- La ley o el mandato jurídico contendrá disposiciones sobre el período de vigencia de los datos obtenidos, recopilados, almacenados y/o gestionados como pruebas por medios electrónicos, que establezcan una equivalencia con las prácticas usuales en la gestión de las pruebas no electrónicas.
- La ley o el mandato jurídico estipulará que el sector público utilice de medios para fomentar la transparencia en lo que respecta a los recursos y herramientas disponibles que puedan facilitar la instauración de la prueba por medios electrónicos.
- La ley o el mandato jurídico garantizará que la recopilación y gestión de pruebas por medios electrónicos se rija en todo momento por los principios de seguridad, eficiencia y eficacia.
- Se deberán establecer políticas públicas que fomenten la cooperación institucional para la elaboración de aplicaciones que utilicen la prueba por medios electrónicos con miras a una mayor automatización de los servicios públicos por medios electrónicos.

.../...

Sección I

- La ley o el mandato jurídico definirá las directrices relativas al principio de neutralidad tecnológica, como forma de ofrecer flexibilidad cuando se elaboren instrumentos y mecanismos relacionados con la prueba por medios electrónicos.
- Cuando proceda, la ley establecerá en qué circunstancias se considera que las versiones impresas (''copias en papel'') de los documentos electrónicos cumplen los requisitos de la regla de ''la mejor prueba''.
- La ley dispondrá que la admisibilidad de la prueba por medios electrónicos se rija por los principios de equivalencia funcional, precaución y acreditación.
- La ley dispondrá que, en la sustanciación del proceso con pruebas por medios electrónicos, se emplee la informática forense.
- La ley regulará en qué circunstancias se establecerá la presunción de integridad de un sistema de registros electrónicos por medio de una declaración jurada, hecha sobre la base de los conocimientos y la convicción de los que declaran, y estipulará la posibilidad de que estos puedan ser sometidos a contrainterrogatorio.
- La ley impondrá sanciones a toda persona que, en una declaración jurada o certificación, haga una afirmación a sabiendas de que es falsa o que a su juicio no es cierta.
- La ley establecerá los criterios de armonización de las sanciones contra una persona que haya hecho afirmaciones falsas en una declaración jurada o un certificado relativo a la integridad de un sistema de registros electrónicos.
- La ley o el mandato jurídico contemplará el establecimiento de procedimientos apropiados de allanamiento e incautación que garanticen la integridad de las pruebas recopiladas.
- La ley o el mandato jurídico contemplará el establecimiento de procedimientos para la certificación y la presentación de los datos obtenidos, así como el entorno digital en el momento de la recopilación de los datos.
- La ley contemplará el reconocimiento de los acuerdos privados sobre admisibilidad de registros electrónicos (y puede extenderlo a los procesos penales, sujeto a restricciones).
- La ley dispondrá que las partes tienen libertad para acordar el uso de un método de firma electrónica, salvo cuando la ley disponga otra cosa.
- La ley dispondrá que una persona que confíe en una firma electrónica deberá asumir las consecuencias jurídicas si no adoptó las medidas razonables para verificar la fiabilidad de esa firma electrónica.
- La ley dispondrá que el proveedor de servicios de certificación mantenga disponibles durante un tiempo los registros de rastreo de los procedimientos de seguridad que utilizó.
- La ley dispondrá que la autoridad de certificación tendrá la facultad y la obligación de certificar también la fecha y hora de los registros electrónicos (''servicio de indicación de tiempo'').

4. LOS PA ÍSES DE LA CARICOM/DEL CARIFORUM PROPORCIONARÁN UNA PROTECCIÓN ADECUADA A LA PRUEBA POR MEDIOS ELECTRÓNICOS

- Se definirá el concepto de ''representación óptica'' a los efectos de la protección de la prueba por medios electrónicos.
- La ley o el mandato jurídico estipulará que se protegerá a las personas contra los prejuicios relativos a la admisibilidad administrativa o judicial de la prueba por medios electrónicos.
- La ley o el mandato jurídico establecerá el reconocimiento del uso de la indicación de tiempo de los certificados electrónicos.
- La ley o el mandato jurídico establecerá el reconocimiento de las normas de procedimiento en el examen de la fiabilidad de los datos contenidos en un sistema de registros electrónicos específico.
- La ley o el mandato jurídico establecerá también, posiblemente a través de reglamentos, los límites del uso legal o ilegal de tecnologías como la criptografía, la esteganografía y el reenvío automático de mensajes (*re-mailing*) en relación con la prueba por medios electrónicos.
- La ley o el mandato jurídico establecerá el reconocimiento de las imágenes como prueba por medios electrónicos, y proporcionará directrices para diferenciar entre imagen electrónica y ''representación óptica''.
- Se aplicarán políticas públicas para fomentar el uso de la certificación de los atributos en los certificados de firma digital para mejorar la capacidad de identificación de su titular y generar pruebas por medios electrónicos.
- La ley o el mandato jurídico alentará el empleo de técnicas seguras (por ejemplo, la transmisión segura a través de IP) cuando se use la videoconferencia en los servicios públicos (por ejemplo, en determinadas audiencias que se lleven a cabo durante las actuaciones judiciales).
- La ley o el mandato jurídico alentará y reconocerá el uso adecuado de cámaras como forma de generar pruebas por medios electrónicos.
- La ley o el mandato jurídico alentará y reconocerá las facilidades que pueden ofrecer los dispositivos de telecomunicaciones para generar pruebas por medios electrónicos.

5. LOS PAÍSES DE LA CARICOM/DEL CARIFORUM ESTABLECERÁN AL MISMO TIEMPO EL MARCO DE LA PRUEBA POR MEDIOS ELECTRÓNICOS Y LAS POLÍTICAS PÚBLICAS SOBRE LOS ASUNTOS CONEXOS

- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas en materia de seguridad nacional.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas en materia de ciberdelincuencia.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas en materia de interceptación de la comunicación.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre preservación inmediata.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre la orden de presentación.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre allanamiento e incautación.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre recopilación de pruebas en tiempo real.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre firma digital.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre privacidad y protección de datos.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre seguridad de la información.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre propiedad intelectual.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas en materia de libertad de la información.
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con los tratados sobre reconocimiento mutuo de los documentos públicos oficiales (de conformidad con el Convenio de La Haya).
- La ley o el mandato jurídico reglamentará el uso de la prueba por medios electrónicos de forma coherente con las políticas públicas sobre inclusión social digital.

Sección II:
Modelo de texto legislativo –
La prueba por medios electrónicos

A continuación se presenta el modelo de texto legislativo que un país puede tomar en consideración cuando elabore de una legislación nacional sobre la prueba por medios electrónicos en el comercio electrónico. Este modelo de texto se basa en el modelo de directrices para políticas expuesto *supra*.

Organización de los artículos

PARTE I – OBSERVACIONES PRELIMINARES

Título abreviado 1. Esta Ley podrá citarse como Ley de la prueba por medios electrónicos, y entrará en vigor [xxx / después de la publicación en el [nombre de la publicación].

Definiciones 2. (1) Por ''certificado acreditativo'' se entiende un certificado expedido por un proveedor acreditado de servicios de certificación.

(2) Por ''destinatario'', en relación con un registro electrónico, se entiende una persona designada por el emisor de dicho registro para que lo reciba, lo que no incluye a ninguna persona que actúe como intermediario con respecto a ese registro electrónico.

(3) Por ''firma electrónica avanzada'' se entiende la firma electrónica suministrada por un proveedor acreditado de servicios de certificación.

(4) Por ''productos o servicios de autenticación'' se entiende los productos o servicios concebidos para identificar al titular de una firma electrónica frente a otras personas.

(5) Por ''certificado'' se entiende una declaración por medios electrónicos que establece el nexo entre los datos de verificación de una firma y una persona, y confirma la identidad de la misma, o el nexo entre los datos de verificación temporal y un registro electrónico, o una comunicación electrónica, y confirma la fecha y hora de los mismos.

(6) Por ''ordenador/computador'' se entiende cualquier sistema de información digital formado por un equipo y programas, destinado a la creación, grabación, almacenamiento, tratamiento y/o transmisión de datos, lo que incluye a cualquier ordenador/computador, dispositivos informáticos, o cualquier otro dispositivo electrónico de información o comunicación concebidos para llevar a cabo esas funciones.

(7) Por ''datos sobre contenido'' se entiende todos aquellos datos, ya sean digitales, ópticos o de otro tipo, incluidos los metadatos, que transmiten esencia, sustancia, información, significado, propósito, intención o información sensible, ya sea de forma individual o combinada, en su estado natural o tratados. Los datos sobre contenido incluyen todos los datos que transmiten el significado o sustancia de una comunicación, así como los datos tratados, almacenados o transmitidos por programas informáticos.

(8) Por ''servicio de criptografía'' se entiende todo servicio que se proporciona al emisor o destinatario de una comunicación electrónica, o a cualquiera que almacene una comunicación electrónica, y está diseñado para facilitar el uso de técnicas de criptografía que garanticen:

(a) que sólo ciertas personas pueden acceder a los datos o la comunicación electrónica, o exponerlos de forma inteligible;

(b) que se puede establecer la autenticidad o integridad de los datos o la comunicación electrónica;

(c) la integridad de los datos o la comunicación electrónica; o

(d) que se puede determinar correctamente la fuente de los datos o la comunicación electrónica.

(9) Por ''datos'' (o ''datos informáticos'', o ''datos electrónicos'') se entiende toda representación de hechos, información o conceptos en una forma adecuada para su tratamiento en un sistema de información, lo que incluye cualquier programa diseñado para hacer que un sistema de información ejecute una función.

(10) Por ''firma digital'' se entiende una firma electrónica basada en criptografía asimétrica, que incluye las claves públicas y privadas asociadas.

(11) Por ''electrónico'' se entiende todo lo que se crea, graba, transmite o almacena en formato digital u otra forma intangible por medios electrónicos, magnéticos, ópticos o cualquier otro medio que permita, como los anteriores, la creación, grabación, transmisión o almacenamiento.

(12) Por ''agente electrónico'' se entiende un programa, ordenador/computador u otro medio electrónico o automatizado, configurado y habilitado por una persona, que se utiliza para iniciar o responder a un registro o evento electrónico, en su totalidad o en parte, sin participación de una persona física.

(13) Por ''autenticación electrónica'' se entiende todo procedimiento empleado con el propósito de verificar que una comunicación electrónica se corresponde con la transmitida por el emisor y no ha sido alterada durante la transmisión.

(14) Por ''comunicación electrónica'' se entiende cualquier transferencia de registros por medio de signos, señales, textos escritos, imágenes, sonidos, datos o información de cualquier naturaleza transmitidos en su totalidad o en parte a través de un sistema alámbrico, radioeléctrico, electromagnético, fotoeléctrico o fotoóptico que afecte al comercio interestatal o extranjero, con exclusión de:

(a) cualquier comunicación telefónica o telegráfica;

(b) cualquier comunicación efectuada a través de un dispositivo de localización por señal acústica;

(c) cualquier comunicación desde un dispositivo de rastreo.

(15) Por ''registro electrónico'' se entiende un conjunto de datos creado, generado, grabado, almacenado, tratado, enviado, comunicado y/o recibido, en cualquier soporte físico, por un ordenador/computador u otro dispositivo similar, y que una persona puede leer o percibir por medio de un sistema informático u otro dispositivo similar, en una pantalla, una versión impresa u otra forma de presentación de esos datos.

(16) Por ''firma electrónica'' se entiende cualquier firma basada en un proceso electrónico, incluyendo la firma digital y la biométrica, entre otras.

(17) Por ''sistema de información'' (o ''sistema informático'', o ''sistema de tratamiento de datos'') se entiende un dispositivo o grupo de dispositivos interconectados o relacionados, entre ellos Internet, en el que uno o varios de esos dispositivos ejecuta, conforme a un programa, un tratamiento automatizado de datos u otra función.

(18) Por ''derecho'' se entiende el *common law*, la legislación y la legislación subordinada.

(19) Por ''procedimiento jurídico'' se entiende un procedimiento civil, penal o administrativo celebrado en un tribunal o ante un juzgado, junta o comisión.

(20) Por ''datos sobre ubicación'' se entiende cualquier dato tratado en una red de comunicaciones electrónicas que indica la ubicación geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas de acceso público.

(21) Por ''emisor'', en relación con un registro electrónico, se entiende una persona que:

(a) envía un registro electrónico;

(b) da instrucciones a otra para que envíe un registro electrónico en su nombre; o

(c) tiene un registro electrónico enviado por su agente electrónico, pero sin incluir a ninguna persona que actúe como agente o intermediario en el envío de ese registro electrónico.

(22) ''Organismo público'' incluye:

(a) un ministerio o departamento del Gobierno;

(b) compañías o empresas de propiedad estatal, total o parcialmente;

(c) órganos que ejercen autoridad por ley, que pueden ser de carácter legislativo, ejecutivo o judicial;

(d) autoridades públicas subnacionales o locales, incluidos los municipios.

(23) Por ''registro'' se entiende cualquier información grabada que ha sido recopilada, creada o recibida durante el inicio, proceso o finalización de una actividad y que cuenta con suficiente contenido, contexto y estructura como para dar cuenta o servir de prueba de dicha actividad o de una transacción, que está inscrita, almacenada o conservada de otro modo en un medio tangible o almacenada en un medio electrónico o de otro y tipo y que es accesible a través de la percepción.

(24) Por ''procedimiento de seguridad'' se entiende un procedimiento, establecido por ley o mediante un acuerdo o adoptado por las partes con pleno conocimiento de causa, que se aplica a los efectos de verificar que una firma, comunicación o acto en formato electrónico pertenece a una persona en particular, o bien para detectar cambios o errores en el contenido de una comunicación electrónica.

(25) El término ''firma'' incluye cualquier símbolo establecido o adoptado, o cualquier metodología o procedimiento utilizado o adoptado por una persona con la intención de autenticar un registro, lo que incluye los métodos electrónicos o digitales.

(26) Por ''datos de creación de una firma'' se entiende los datos originales, tales como códigos o claves privadas de criptografía, empleados por el firmante para crear una firma electrónica.

(27) Por ''información de abonado'' se entiende cualquier información, contenida en forma de dato informático o en cualquier otra forma, de la que está en posesión un proveedor de servicios y que tiene relación con sus abonados, con exclusión de los datos sobre tráfico o sobre contenido, y que permite establecer:

(a) el tipo de servicio de comunicación utilizado, las disposiciones técnicas relacionadas con el mismo y el periodo de servicio;

(b) la identidad, dirección postal o geográfica, número de teléfono de contacto, e información sobre facturación y pagos del abonado, tal como figura en el contrato o acuerdo de servicio; y/o

(c) la ubicación del equipo de comunicación, tal como figura en el contrato o acuerdo de servicio.

(28) Por ''datos sobre tráfico'' se entiende aquellos datos informáticos que:

(a) se refieren a una comunicación realizada por medio de un sistema informático;

(b) son generados por un sistema informático que forma parte de la cadena de comunicación; y

(c) muestran el origen, destino, encaminamiento, fecha y hora, tamaño o duración de la comunicación, así como el tipo de servicios que la sustentan.

PARTE II – ADMISIBILIDAD

Modificación de la autenticación y la regla de la mejor prueba

3. Esta Ley no modifica ninguna disposición basada en el *common law* o el derecho positivo en relación con la admisibilidad de los registros, salvo las relativas a la autenticación y la regla de la mejor prueba.

Disposiciones del *common law* y el derecho positivo

4. En la aplicación de una disposición basada en el *common law* o el derecho positivo en relación con la admisibilidad de los registros, el tribunal podrá tener en cuenta los principios que rigen la admisibilidad de los registros electrónicos según lo dispuesto en la presente Ley.

Admisibilidad general de la prueba por medios electrónicos

5. Ninguna disposición en las reglas sobre pruebas se utilizará para denegar la admisibilidad de un registro como prueba por el mero hecho de ser electrónico.

Aplicación de la regla de la mejor prueba

6. (1) En cualquier procedimiento jurídico, sin perjuicio de lo que figura en el párrafo 2 *infra*, cuando se aplique la regla de la mejor prueba en materia de registro electrónico, se considerará que esta regla se cumple si se demuestra la integridad del ordenador/computador en el que, o a través del cual, se grabaron o almacenaron los datos.

(2) A menos que se demuestre lo contrario, en cualquier procedimiento jurídico se presumirá la integridad del ordenador/computador en que se grabó o almacenó un registro electrónico:

(a) cuando se presenten pruebas de que el sistema informático u otro dispositivo similar funcionó correctamente en todo momento, o de no ser así, que su funcionamiento incorrecto en algunos aspectos o su falta de funcionamiento, no afectó a la integridad del registro, y que no hay otros motivos razonables para dudar de dicha integridad;

(b) cuando se establezca que el registro electrónico fue grabado o almacenado por una parte que tiene un interés opuesto al de la parte que trata de introducirlo en un procedimiento; o

(c) cuando se establezca que el registro electrónico fue grabado o almacenado en el curso normal y ordinario de las actividades por una persona que no es parte en el procedimiento y que lo grabó o almacenó sin control de la parte que pretende introducirlo.

Integridad de la información y reglas específicas de admisibilidad

7. (1) Una declaración contenida en un registro electrónico producido por un ordenador/computador que sólo sea un rumor no se admitirá en ningún procedimiento como prueba de un hecho invocado, a menos que se presuma la integridad del ordenador/computador en virtud del párrafo siguiente.

(2) A menos que se demuestre lo contrario, en cualquier procedimiento jurídico se presumirá la integridad de un ordenador/computador en que se grabe o almacene un registro electrónico, si el registro de la transacción:

(a) ha permanecido completo e inalterado, como no sea :

(i) el añadido de una manifestación de respaldo; o

(ii) un cambio inmaterial;

surgidos en el curso normal de la comunicación, el almacenamiento o la visualización;

(b) ha sido certificado o firmado por vía electrónica mediante un método suministrado por una entidad de certificación acreditada;

(c) ha sido certificado por un notario en cuanto a su integridad y contenido;

(d) ha sido grabado en un dispositivo de almacenamiento no modificable, o en cualquier otro medio electrónico que no permite la alteración de los registros electrónicos;

(e) ha sido examinado por un experto designado por el tribunal que ha verificado su integridad; o

(f) en relación con el cual:

(i) se presenten pruebas de que el sistema informático u otro dispositivo similar funcionó correctamente en todo momento, o de no ser así, que su funcionamiento incorrecto en algunos aspectos o su falta de funcionamiento, no afectó a la integridad del registro, y que no hay otros motivos razonables para dudar de dicha integridad;

(ii) se establezca que el registro electrónico fue grabado o almacenado por una parte que tiene un interés opuesto al de la parte que trata de introducirlo en un procedimiento; o

(iii) se establezca que el registro electrónico fue grabado o almacenado en el curso normal y ordinario de las actividades por una persona que no es parte en el procedimiento y que lo grabó o almacenó sin control de la parte que pretende introducirlo.

(3) Cuando una declaración contenida en un registro electrónico producido por un ordenador/computador no constituya un rumor, se admitirá como prueba si se cumplen respecto de ese registro las condiciones especificadas en el párrafo 2 *supra*.

Versiones impresas

8. En un procedimiento jurídico, cuando de forma manifiesta y constante se ha actuado sobre la base de un registro electrónico en forma impresa, se lo ha usado como fundamento de algo, o se lo ha utilizado como registro de la información grabada o almacenada, esa versión impresa será considerada registro a los efectos de la regla de la mejor prueba.

La carga de probar la autenticidad de la prueba por medios electrónicos

9. La persona que trata de introducir un registro electrónico en un procedimiento jurídico tiene la carga de probar su autenticidad mediante elementos que justifiquen que dicho registro es lo que esa persona alega. En caso de que exista una legislación especial para proteger a las personas más vulnerables, como los consumidores y los niños, y que establezca una asignación de la carga de prueba más favorable a estas personas, dicha legislación tendrá prioridad sobre este artículo.

Normas

10. A los efectos de determinar, en virtud de otra ley, si un registro electrónico es admisible, se pueden presentar pruebas en relación con cualquier norma, procedimiento, uso o práctica de grabación o conservación de registros electrónicos, teniendo en cuenta el tipo de negocio o empresa que usó, grabó o conservó el registro electrónico y la naturaleza y finalidad de ese registro. Las autoridades públicas encargadas de elaborar o aprobar las normas técnicas o procedimientos de seguridad pertinentes establecerán las directrices para orientar sobre los criterios que se deben aplicar para cumplir con este artículo.

Declaraciones juradas

11. Cuando se pretenda invocar un registro electrónico como prueba, se lo podrá presentar en forma de declaración jurada.

Acuerdo sobre la admisibilidad de la prueba

12. (1) Salvo que otra ley prevea otra cosa, un registro electrónico es admisible, sin perjuicio de lo que decida el tribunal, si en algún momento las partes en el procedimiento han acordado expresamente que no se podrá impugnar su admisibilidad.

(2) No obstante lo establecido en el párrafo 1, un acuerdo entre las partes sobre la admisibilidad de un registro electrónico presentado por la acusación en un procedimiento penal no tendrá validez si en el momento del acuerdo el acusado, o cualquiera de los acusados, no estaba legalmente asistido o representado.

Firma electrónica

13. (1) Una firma electrónica no dejará de tener fuerza y efecto jurídicos por el mero hecho de estar en formato electrónico.

(2) Una firma electrónica se puede probar de varias maneras, entre otras cosas, demostrando que, con arreglo a un procedimiento existente, la persona, para llevar a cabo una transacción, debía haber utilizado un símbolo u otro procedimiento de seguridad para verificar que ese registro electrónico correspondía al de la persona.

Requisitos de firma electrónica

14. (1) Cuando la ley requiera la firma de una persona, este requisito se podrá cumplir con una firma electrónica, si la firma electrónica que se emplea es suficientemente fiable y adecuada para el propósito para el que se generó o comunicó, en todas las circunstancias, con inclusión de los acuerdos pertinentes.

(2) El párrafo 1 se aplicará cuando el requisito de una firma se presente como obligación o la ley prevea consecuencias en caso de ausencia de firma.

(3) Las partes podrán convenir en utilizar un método determinado de firma electrónica, salvo cuando la ley disponga otra cosa.

(4) Cuando las partes de una transacción electrónica requieran una firma electrónica, y no se han puesto de acuerdo sobre el tipo de firma electrónica que se utilizará, se considerará que dicho requisito se cumple en relación con el mensaje de datos si:

(a) los datos de creación de la firma están vinculados al firmante y no a otra persona;

(b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control del firmante y no de otra persona;

(c) no se detecta ninguna alteración de la firma electrónica posterior al momento de la firma; y

(d) cuando el propósito del requisito jurídico de la firma es garantizar la veracidad de la información a que se refiere, una alteración de esa información posterior al momento de la firma podría detectarse

(5) El párrafo 4 no limita la capacidad de una persona para:

(a) establecer en cualquier otra forma la fiabilidad de una firma electrónica con el propósito de satisfacer el requisito previsto en el párrafo 1, o

(b) aportar pruebas de la falta de fiabilidad de una firma electrónica.

(6) Una persona que confíe en una firma electrónica, sin tomar las medidas razonables para verificar la fiabilidad de la misma, deberá asumir las consecuencias jurídicas que se puedan derivar de esa omisión.

(7) El tribunal tendrá en cuenta toda ley que contemple la verificación del autor y la integridad de los registros electrónicos con firma digital.

Técnicas y procedimientos alternativos para la presentación de pruebas por medios electrónicos

15. Además de los medios probatorios que se indican en las secciones anteriores de esta Ley, se pueden presentar pruebas electrónicas en relación con un registro electrónico mediante otras técnicas y procedimientos alternativos, tales como la certificación por notarios públicos, jueces de paz u otras autoridades competentes; la grabación del registro en un soporte que no pueda modificarse; y la informática forense en el transcurso de la sustanciación del proceso.

PARTE III – DISPOSICIONES GENERALES

Admisibilidad de registros electrónicos de otros países

16. Cuando la prueba por medios electrónicos se origine en otra jurisdicción, su admisibilidad no se verá afectada si se demuestra o se presume la integridad del ordenador/computador asociado a dicha prueba, de conformidad con las disposiciones previstas en los artículos 6, párrafo 2 a), y 7, párrafo 2, de la presente Ley.

Reconocimiento de firmas y documentos electrónicos extranjeros

17. (1) Para determinar si una información en formato electrónico tiene efectos jurídicos o no, o en qué medida, no se tendrá en cuenta su lugar de creación o uso, ni el lugar de la actividad en que se creó, siempre que el registro electrónico se encuentre en la jurisdicción nacional.

(2) Cuando el registro electrónico se encuentra en una jurisdicción extranjera, el párrafo 1 *supra* no se aplicará, a menos que:

(a) la parte que invoca la prueba de los contenidos del registro electrónico haya entregado a la otra parte, al menos 14 días antes de la fecha en que se invoque la prueba, una copia del registro electrónico que se propone presentar;

(b) el tribunal determine que es aplicable; o

(c) exista un tratado internacional en vigor que establezca el reconocimiento de los registros o firmas electrónicos ubicados en jurisdicciones extranjeras.

Interpretación de conformidad con los principios internacionalmente aceptados

18. Las disposiciones de esta Ley se interpretarán y aplicarán a la luz de los principios internacionalmente aceptados de neutralidad tecnológica y equivalencia funcional.

Reglamentos

19. El Ministro podrá elaborar reglamentos para dar efecto a los objetivos de esta Ley y prescribir cualquier acción que esta ley requiera o autorice que se prescriba. Al hacerlo, el Ministro podrá considerar las mejores prácticas y normas a nivel internacional.

Sección III:
Notas explicativas del modelo de texto legislativo sobre la prueba por medios electrónicos

INTRODUCCIÓN

1. Este texto legislativo elabora un marco jurídico para la admisibilidad de los registros electrónicos. Los principales objetivos de este texto legislativo (Ley) son: establecer la admisibilidad de la prueba por medios electrónicos en general; modificar las normas jurídicas de la autenticación y de la mejor prueba; determinar los criterios del proceso para establecer la presunción de integridad de los ordenadores/computadores y los registros electrónicos; abordar la cuestión de la carga de prueba correspondiente; regular la admisibilidad de la firma electrónica; determinar la interpretación basada en los principios aceptados internacionalmente; y contemplar el reconocimiento de los registros electrónicos originados o ubicados en otros países.

2. Las presentes notas apuntan a explicar el contenido de esta Ley, y deberán leerse conjuntamente con ella. Se explica la importancia de las principales disposiciones de la Ley y, si es pertinente, se señalan a la atención los debates concretos celebrados por el grupo de trabajo, destacando las diferentes opciones de regulación examinadas. No dan, ni pretenden dar, una descripción detallada de la presente Ley. Por lo tanto, cuando un artículo o párrafo de artículo no parece precisar de aclaraciones, comentarios o referencias exhaustivas, o cuando no hubo debate sobre una disposición en particular, no se da ninguna explicación detallada.

3. Esta Ley consta de tres partes:

   - La **Parte I** contiene definiciones;
   - La **Parte II** modifica las normas jurídicas de la autenticación y de la mejor prueba, establece el principio de no discriminación de los registros electrónicos, reglamenta la aplicación de la regla de la mejor prueba, define los criterios para establecer la presunción de integridad de los ordenadores/computadores y los registros electrónicos, asigna la carga de prueba, determina el establecimiento de directrices sobre el cumplimiento de las normas técnicas y los procedimientos de seguridad, admite los acuerdos sobre admisibilidad de pruebas por medios electrónicos en los procesos judiciales, reconoce la firma electrónica como prueba, y aborda las técnicas y procedimientos alternativos para la presentación de pruebas por medios electrónicos;
   - **La Parte III** establece las disposiciones generales que contemplan la admisibilidad de los registros electrónicos de otros países, el reconocimiento de firmas y documentos electrónicos extranjeros, la interpretación de acuerdo con los principios internacionalmente aceptados, y posibles regulaciones en consonancia con las mejores prácticas y normas a nivel internacional.

COMENTARIO SOBRE LOS ARTÍCULOS

PARTE I – OBSERVACIONES PRELIMINARES

4. La Parte I contiene disposiciones preliminares, como el título abreviado y la cláusula de inicio en el **Artículo 1**, y las definiciones en el **Artículo 2**.

5. La Parte I ha suscitado un debate dentro del grupo de trabajo con respecto al estilo de formulación según las distintas jurisdicciones. Se discutió si se debería añadir un artículo que describiera los objetivos de esta Ley, y se llegó al acuerdo de que esta cuestión se dejara a discreción de cada Estado beneficiario.

Artículo 2. Definiciones

6. La definición de **ordenador/computador** contenida en el párrafo 6 *supra* deja margen para abarcar todos los dispositivos electrónicos que puedan ejecutar las funciones típicas de los ordenadores/computadores.

7. Hubo un debate dentro del grupo de trabajo sobre si debía incluirse una referencia explícita al equipo de telecomunicaciones como los teléfonos móviles inteligentes. Se acordó que el rápido ritmo del progreso tecnológico, junto con el principio de neutralidad tecnológica, hacen aconsejable mantener la expresión general de ''dispositivos electrónicos de información o comunicación'' como complemento a los términos ''ordenador/computador'' y ''dispositivos informáticos''.

8. Los **datos sobre contenido** (junto con los datos sobre ubicación y los datos sobre tráfico, que se definen en los párrafos 20 y 28, respectivamente) son datos cuya generación, comunicación, tratamiento y almacenamiento se prestan naturalmente a la presentación de pruebas por medios electrónicos, ya que son consustanciales a las comunicaciones y transacciones subyacentes.

9. La definición de ''datos sobre contenido'' está redactada de manera que abarque cualquier contenido posible de un registro electrónico (''esencia, sustancia, información, significado, propósito, intención o información sensible'').

10. Esta definición se refiere a datos sobre contenido que han sido tratados y sin tratar. El objetivo era abarcar no sólo los contenidos ''en bruto'' destinados a ser transformados durante el tratamiento de datos, sino también los diferentes datos generados como resultado de esa actividad de tratamiento

11. Dicha definición se refiere también a los ''metadatos'', una segunda capa que contiene ''datos sobre datos'' (como el lenguaje utilizado para escribir algunos contenidos, la fecha y hora de su generación, dónde encontrar más información acerca de esos contenidos, etc.). Dado que el uso de metadatos y de metaetiquetas está cada vez más difundido (debido, sobre todo, a la utilización común de los motores de búsqueda en Internet impulsada por esos metadatos y metaetiquetas), los metadatos pueden proporcionar elementos importantes para la presentación de pruebas por medios electrónicos relativas a los datos sobre contenido.

12. Los **datos** se definen en el párrafo 9 como ''toda representación de hechos, información o conceptos en una forma adecuada para su tratamiento en un sistema de información''.

13. Se prefirió la expresión ''datos'' a la expresión ''información'', que figura en la legislación de algunos países en relación con la prueba en general, pero no necesariamente con la prueba por medios electrónicos. Como el alcance de esta Ley se refiere únicamente a la prueba por medios electrónicos, la intención era resaltar sólo los hechos, información y conceptos representados en formato electrónico, o sea, en forma de dígitos binarios.

14. El grupo de trabajo debatió sobre la conveniencia de incluir o no la expresión ''estado'' en esta definición, lo que serviría para destacar en que los datos pueden concebirse de forma lógica no sólo como una sucesión de dígitos ''0'' y ''1'' (que representan letras o números), sino también como cambios tangibles del estado electromagnético u óptico en un ordenador/computador que el sistema de información ''lee'' como correspondiente respectivamente a los dígitos binarios. Aunque la expresión ''estado'' puede ayudar a que los profanos (incluidos los magistrados) tengan en cuenta también el aspecto tangible de los datos y a que se los califique jurídicamente como ''cosa'' (para establecer que pueden ser objeto de posesión o de apropiación indebida, entre otros fines), la última parte de esa definición, cuando dice ''lo que incluye cualquier programa diseñado para hacer que un sistema de información ejecute una función'', puede indirectamente lograr, en cierta medida, el objetivo de representar los datos de una forma tangible (pues se prevé que, como resultado de la actividad de un sistema de información, se produzca un cambio tangible). Por tanto, se deja a discreción de los Estados beneficiarios la posibilidad de determinar en qué grado se hará hincapié en el aspecto tangible de los datos.

15. Finalmente, dicha definición deja claro que ''datos'' es sinónimo de ''datos informáticos'' y de ''datos electrónicos'', expresiones presentes en la legislación respectiva de los países y a nivel internacional. En consecuencia, la correspondencia entre estas legislaciones está garantizada, en aras de la coherencia, especialmente en lo que respecta a la legislación de otros países, donde hay una mayor diversidad en la terminología empleada, y se acentúa la necesidad de establecer puentes que faciliten la interpretación y la aplicación común.

16. La **firma digital** se ha definido en el párrafo 10 como un tipo particular de firma electrónica. Junto con la definición de otras expresiones (como **certificado acreditativo**, **firma electrónica avanzada**, **productos y servicios de autenticación**, **certificado**, **servicio de criptografía**, **firma electrónica**, **firma** y **datos de creación de una firma)** que aparecen en otros párrafos del Artículo 2, aporta un significado coherente a un sistema fundamental de presentación de pruebas por medios electrónicos, a saber, el sistema de autenticación, certificación y acreditación de la firma digital, que permite identificar el autor, el origen, la fecha y hora, y otros elementos de esa firma.

17. Las definiciones aprobadas para este conjunto de expresiones tienen en cuenta que el Estado beneficiario puede haber establecido o no una tecnología o una organización determinada para construir un sistema de certificación de firma electrónica, ya sea a nivel nacional o contratado en el extranjero. Por esa razón, las definiciones se han centrado en los aspectos básicos, dejando para una regulación ulterior las posibles opciones más específicas (por ejemplo, la diferente estructura de las funciones y atribuciones, la asignación de recursos regionales o nacionales, etc.).

18. Al adoptar este enfoque, la definición de firma digital facilita la integración con otras disposiciones de esta Ley, como las relativas al cumplimiento con la regla de la mejor prueba o los medios alternativos de presentación de pruebas electrónicas, puesto que la flexibilidad que ofrece el texto genérico aprobado permite adaptarla a diferentes formas de utilización de la firma digital para demostrar la integridad y fiabilidad de un ordenador/computador o de un registro electrónico, o para reproducir o incorporar formas alternativas de prueba por medios electrónicos.

19. Lo que caracteriza al **agente electrónico**, tal como se define en el párrafo 12, es la respuesta electrónica automatizada que se utiliza como interfaz para la interacción de los seres humanos con los ordenadores/computadores. Esta definición es uno de los elementos que integra los conceptos de emisor y destinatario de una comunicación electrónica, y puede determinar si el envío o la recepción ha tenido lugar efectivamente, y cómo y dónde quedaría demostrado.

20. La fiabilidad de las comunicaciones realizadas con medios electrónicos es fundamental para generar las pertinentes pruebas por medios electrónicos. El concepto de **autenticación electrónica**, definido en el párrafo 13, ayuda a determinar los procedimientos que se pueden utilizar para comprobar si una comunicación ha sido alterada durante la transmisión, así como establecer quién fue su emisor.

21. La definición de **comunicación electrónica**, contenida en el párrafo 14, es importante, ya que se centra en la transferencia de registros, que incluye el envío y la recepción, mientras que las definiciones de ''ordenador/computador'' o de ''sistema de información'' se limitan a la actividad interna del ordenador/computador o del sistema de información.

22. El grupo de trabajo ha debatido sobre la conveniencia o no de incluir la referencia a ''cualquier comunicación telefónica o telegráfica''. Se expresó cierta inquietud en el sentido de que tales expresiones podrían solaparse con las ya existentes en las leyes de telecomunicaciones de algunos países, especialmente con respecto a la telefonía, y los dispositivos de localización y de rastreo. El grupo decidió que se debía dejar a discreción del Estado beneficiario la posibilidad de mantener o no esta formulación.

23. El párrafo 15 define **registro electrónico** como un conjunto de datos que una persona puede leer o percibir por medio de un sistema informático u otro dispositivo similar.

24. Mientras que los datos se representan en forma binaria para ser ''leídos'' por un ordenador/computador o ''traducidos'' por un programa informático, el registro electrónico es la representación o resultado que muestra un sistema de información y que puede ser percibido por un ser humano.

25. La distinción entre esas expresiones complementarias, ''datos'' y ''registro electrónico'', es necesaria para legislar sobre la prueba por medios electrónicos, ya que la prueba sobre algunos hechos, informaciones o conceptos puede basarse en la percepción de una persona (o en la capacidad de ser percibidos por ella) y no sólo en la posibilidad de indagación del aspecto técnico.

26. La definición de ''registro electrónico'' presenta también interés para determinar el significado de ''dispositivo electrónico de información'' (que ha sido mencionado en algunas disposiciones de esta Ley como ''dispositivos electrónicos de información o comunicación''), ya que claramente apunta a denotar un dispositivo utilizado por seres humanos para acceder a registros electrónicos o aprehenderlos por medio de la percepción.

27. Además, la definición de ''registro electrónico'' incorpora la expresión ''en cualquier soporte físico'', que debería contribuir a ampliar el alcance de los medios relacionados con los registros electrónicos, más allá de los medios de comunicación tradicionales, para abarcar, por ejemplo, los medios biométricos (como la evaluación de las huellas dactilares o del iris), que se están aplicando cada vez más en el contexto de la prueba por medios electrónicos.

28. Del mismo modo, la referencia a las versiones impresas aclara que un registro electrónico no necesariamente debe percibirse en un sistema informático, sino que también puede apreciarse como un elemento externo a él.

29. Igualmente importante para la comprensión de los fenómenos que rodean la prueba por medios electrónicos es la definición de **sistema de información**, contenida en el párrafo 17. Si bien la definición de ''ordenador/computador'' se refiere a un solo equipo electrónico, la definición de ''sistema de información'' comprende grupos de dispositivos interconectados, como es propio de las redes electrónicas.

30. Esta definición tan amplia podría incluir redes de distintos niveles, incluido Internet, que se considera técnicamente una ''red de redes''. Dada la magnitud de Internet como escenario para la producción y recopilación de pruebas por medios electrónicos, mereció una referencia específica. El concepto de grupo de dispositivos interconectados es suficientemente amplio como para abarcar cualquier equipo conectado a Internet.

31. El grupo de trabajo ha debatido si esta Ley debe utilizar la expresión ''sistema informático'' o ''sistema de información''. La balanza se ha inclinado en favor de ''sistema de información'' (y ''sistema de tratamiento de la información''), utilizado en la legislación de la mayoría de los países. Aunque hay algunas diferencias técnicas de significado entre ''sistema de información'' y ''sistema informático'', no se consideraron esenciales en el contexto de la prueba por medios electrónicos, por lo que se aprobó el uso de ''sistema de información'', al tiempo que se añadía ''sistema informático'' y ''sistema de tratamiento de datos'' como expresiones equivalentes. Se dejó a criterio de cada Estado beneficiario fijar el nivel de precisión técnica deseado sobre estos conceptos en el contexto de la presente Ley.

32. La definición de **procedimiento jurídico**, contenida en el párrafo 19, comprende no sólo los procedimientos civiles sino también los penales y administrativos. Mientras que la prueba por medios electrónicos tiende a ser bien asimilada en los procesos civiles, a menudo se cuestiona en los procesos penales, en los que se alega que por su naturaleza ''virtual'' no aporta elementos suficientes para sustentar una condena penal. Asimismo, en el ámbito administrativo los responsables no se ocupan del aspecto ''intangible'' comúnmente asociado con la prueba por medios electrónicos, y dejan para el proceso judicial la tarea de evaluar dicha prueba. Por tanto, es importante dejar claro que una prueba por medios electrónicos presentada de forma adecuada tendrá validez en cualquier procedimiento, con independencia de que sea civil o penal, judicial o administrativo.

33. La ubicación del equipo es un elemento importante en la creación de la prueba, ya que puede dar lugar a diferentes conclusiones y consecuencias, como la atribución de la jurisdicción y de las leyes aplicables, la determinación del nivel de seguridad necesario y la correspondiente responsabilidad, la indicación sobre el emisor de los documentos o de las comunicaciones, la prueba efectiva de su envío o recepción, etc. La definición de los **datos sobre ubicación**, en el párrafo 20, reconoce la importancia de la ubicación geográfica del equipo para la presentación de una prueba en el contexto de las redes de comunicaciones electrónicas.

34. Esta definición ha seleccionado el ''equipo terminal'' como parámetro para la determinación de la ubicación geográfica, ya que esta expresión es suficientemente flexible como para abarcar no slo un ordenador/computador, sino también cualquier otro dispositivo que pueda utilizarse en el contexto de un servicio de comunicaciones electrónicas.

35. También merece destacarse que esta definición limita el alcance de la determinación de la ubicación geográfica a los servicios de comunicaciones electrónicas ''de acceso público'', lo que puede contribuir a equilibrar, por un lado, los motivos de seguridad que apoyan la necesidad de identificar una ubicación geográfica y, por otro y cuando corresponda, el derecho a la privacidad.

36. El concepto de **emisor**, definido en el párrafo 21, es suficientemente amplio como para incluir no sólo a la persona que realmente envía una comunicación electrónica, sino también a la que da instrucciones a otra para que lo haga en su nombre, así como la que utiliza un agente electrónico a esos efectos.

37. La amplitud de este concepto es cada vez más importante dado el rápido crecimiento del volumen de las comunicaciones electrónicas ''enviadas'' a través de terceros (como ''centros de llamadas electrónicos'') o agentes electrónicos (como los llamados ''*web-wrapping agreements*'' o acuerdos de licencia para descargar programas de Internet).

38. El grupo de trabajo ha decidido incluir una observación para aclarar que ''agente electrónico'' no incluye a personas. Dicha observación es coherente con la definición de ''agente electrónico'' que figura en el párrafo 12.

39. El párrafo 22 define **organismo público**, que incluye a cualquier ministerio o departamento gubernamental, empresa de propiedad estatal, órganos que ejercen la autoridad legal, y autoridades públicas a nivel subnacional o local.

40. Esta amplia definición está en consonancia con la de ''derecho'', recogida en el párrafo 18 y que incluye el *common law*, la legislación y la legislación subordinada, y con la observación 17 *supra*, que menciona la posibilidad de una regulación ulterior por la que se establezca un sistema de autenticación y/o certificación de firmas digitales. La cuestión radica en que la prueba por medios electrónicos presenta una amplia gama de consecuencias para los órganos del Estado y para todos los ciudadanos, por lo cual hay una gran diversidad de leyes que la reglamentan, así como un gran número de autoridades o de empresas de propiedad estatal que pueden usarla, o regularla, y la definición pertinente debe ser suficientemente amplia.

41. Aunque en esta Ley no hay un número significativo de disposiciones que utilicen esta definición (o que la utilicen indirectamente, como en el Artículo 10, que se refiere a las ''autoridades públicas''), la Ley predetermina la amplia gama de organismos públicos de los que se espera que emitan o sean beneficiarios de una mayor regulación (como en el ejemplo citado sobre la creación de un sistema de autenticación y/o certificación de firmas digitales), lo que sentaría las bases para una legislación subordinada en el futuro.

42. La definición de **procedimiento de seguridad** contenida en el párrafo 24 va más allá del contenido de las definiciones de ''productos y servicios de autenticación'' y ''autenticación electrónica'', abordadas en los párrafos 4 y 13, respectivamente, en el sentido de que la presunción de integridad de un ordenador/computador se basa en la adopción de procedimientos de seguridad, independientemente de cualquier posible prueba de autenticación electrónica, y que las normas técnicas relativas a la seguridad de la información son básicamente de carácter procesal y no requieren necesariamente del uso de un producto o servicio de autenticación. Por lo tanto, la definición de ''procedimiento de seguridad'' es un ingrediente adicional importante para legitimar la presentación de pruebas por medios electrónicos.

43. El texto de dicha definición incorpora no sólo los procedimientos de seguridad en virtud de las normas técnicas, sino también los establecidos por ley, por convenio o por la práctica común conocida, ya que es importante tener en cuenta la libre voluntad de las partes interesadas para negociar el nivel de los procedimientos de seguridad que se desean, así como las mejores prácticas en este terreno a nivel nacional y/o internacional.

44. **Información del abonado** es un concepto definido en el párrafo 27, que trata de abarcar los datos de inscripción de la persona que contrata un servicio de comunicación electrónica y los datos relativos a documentos o comunicaciones que tengan relación con ese abonado.

45. Los datos de inscripción pueden ser un elemento importante para la presentación de pruebas por medios electrónicos, especialmente en lo que se refiere a las comunicaciones anónimas, que acentúa la necesidad de conocer detalles como el nombre, documento de identidad y dirección del abonado.

46. De manera similar a lo que sucede con la expresión **organismo público**, ''información del abonado'' es un concepto interesante de cara a una mayor reglamentación de la prueba por medios electrónicos (y/o asuntos relacionados con la misma, como la responsabilidad de los proveedores de servicios de Internet, de mantener y facilitar los datos de abonado), por lo que es importante que esta Ley preestablezca una definición que garantice un significado uniforme en su uso posterior.

47. El párrafo 28, que trata de los **datos sobre tráfico**, pretende incluir aquellos datos de interés para la presentación de pruebas por medios electrónicos en cuanto al flujo de las comunicaciones electrónicas. Algunos detalles como el origen, encaminamiento, destino, fecha, hora, tamaño y duración son muy importantes para determinar el autor, el lugar y la fecha y hora de ciertas acciones, especialmente cuando los flujos de la comunicación electrónica se dividen en ''paquetes'' que pueden seguir diferentes caminos hasta llegar a su destino, como sucede en Internet.

Sección III

PARTE II – ADMISIBILIDAD

Artículo 3: Modificación de las reglas de autenticación y de la mejor prueba

48. El objetivo principal de este Artículo es determinar la integración de esta Ley con las disposiciones del *common law* y del derecho positivo que regulan la admisibilidad de los registros, así como aclarar que la presente Ley sólo modifica las disposiciones legales relativas a las reglas de autenticación y de la mejor prueba.

49. Al especificar las leyes que se han modificado, este Artículo automáticamente presupone que las leyes no modificadas por la presente Ley también se aplicarán a los asuntos regulados por la misma. Esos temas se considerarán como un capítulo específico dentro del ámbito de aplicación de los principios más generales de admisibilidad de las pruebas.

Artículo 4: Disposiciones del *common law* y del derecho positivo

50. El objetivo de este artículo es establecer que en la aplicación de las disposiciones del *common law* y del derecho positivo que tratan de la admisibilidad de los registros, los tribunales tendrán en cuenta las disposiciones de esta Ley cuando deban considerar los registros electrónicos. Es importante que los tribunales reconozcan la especificidad de la materia y de las disposiciones previstas en esta Ley, y por ello este Artículo trata de señalar a la atención de los magistrados la necesidad de hacerla cumplir.

Artículo 5: Admisibilidad general de la prueba por medios electrónicos

51. Este Artículo establece el principio de no discriminación de los registros electrónicos. Cualquier registro puede ser fiable como prueba o no, independientemente de que sea electrónico o no. Por lo tanto, no hay ninguna razón para discriminar *a priori* los registros electrónicos. Podría incluso decirse que ciertos registros electrónicos (como es el caso de los certificados de firmas digitales) pueden ser más fidedignos que los registros no electrónicos.

52. La importancia de este Artículo es que establece la admisibilidad de los registros electrónicos como regla general, sin perjuicio de los requisitos enumerados en los Artículos siguientes.

Artículo 6: Aplicación de la regla de la mejor prueba

53. Dado que la regla de la mejor prueba es un principio tradicional del derecho en el sistema del *common law*, es importante que la legislación sobre la prueba por medios electrónicos sea compatible con dicho principio.

54. Con el fin de armonizar la aplicación de este principio con las características de los ordenadores/computadores, este Artículo establece que se considerará que se cumple la regla de la mejor prueba si se demuestra la integridad del ordenador/computador en el que, o a través del cual, se grabaron o almacenaron ciertos datos.

55. La regla de la mejor prueba requiere la presentación de los originales de un documento determinado, pero difícilmente se puede determinar si un dato electrónico es un original o una copia, por lo que la prueba de la integridad de un ordenador/computador es una adaptación, *mutatis mutandis,* de la intención tradicional de la regla de la mejor prueba.

56. Esta adaptación tiene razones jurídicas, técnicas y económicas. Desde el punto de vista jurídico, la filosofía que inspira la regla de la mejor prueba es asegurar que se presentan las pruebas más adecuadas posibles (en general, los originales de algunos documentos). Desde el punto de vista técnico y económico, no es plausible aplicar tecnologías y procedimientos (por ejemplo, certificados de firma digital) que equivalgan a un original en todos los registros electrónicos de un sistema de información. Por consiguiente, la conjunción de razones jurídicas, técnicas y económicas indica que, en circunstancias normales, la mejor prueba posible consiste en demostrar la integridad de un ordenador/computador.

57. En el párrafo 2 se enumeran las situaciones que autorizan la presunción de integridad de un ordenador/computador, que básicamente son: a) cuando se aportan pruebas de que el equipo funcionaba correctamente, b) cuando el registro electrónico fue grabado o almacenado por una parte que tiene un interés opuesto a la parte que trata de introducirlo en un procedimiento, o c) cuando el registro electrónico fue grabado o almacenado por una persona que no es parte en el proceso y que lo grabó o almacenó sin **c**ontrol de la parte que pretende introducirlo. En pocas palabras, esa presunción se aplica cuando existen pruebas del correcto funcionamiento de un ordenador/computador o cuando no hay un interés divergente o sospechoso de la parte que trata de introducir el registro electrónico en un procedimiento.

Artículo 7: Integridad de la información y reglas específicas de admisibilidad

58. La presunción sobre la integridad de los ordenadores/computadores contemplada en términos generales en el Artículo 6 también se aborda en la disposición contenida en el Artículo 7, que reúne en su párrafo 2 una lista de situaciones en las que la integridad de un registro electrónico induce a la presunción de la integridad del ordenador/computador, en cualquier procedimiento jurídico y con independencia de que el registro electrónico constituya o no un rumor (según lo previsto en los párrafos 1 y 3, respectivamente).

59. Dicha lista empieza haciendo referencia a los registros de transacciones (es decir, los registros electrónicos) que han permanecido completos e inalterados, como no sean los cambios inmateriales surgidos en el transcurso normal de la comunicación, almacenamiento o visualización. La formulación del artículo es importante, porque los ordenadores/computadores y registros electrónicos difícilmente pueden ser ''congelados'' y mantenerse inmunes a cualquier tipo de cambio, y porque limita el alcance de los cambios a los que realmente pueden poner en peligro la fiabilidad de un registro electrónico.

60. La segunda situación contemplada se refiere a los registros electrónicos certificados o firmados electrónicamente mediante un método facilitado por entidades de certificación acreditadas. Resulta claramente conveniente establecer autoridades o entidades de certificación acreditadas, ya que esa acreditación ofrece una presunción formal por sí misma y contribuye así a inducir la presunción de la integridad material del registro electrónico.

61. La lista menciona a continuación la posibilidad de certificación de la integridad y el contenido del registro electrónico por parte de un notario, que es otra opción disponible para las partes interesadas y que puede ser de interés en la medida en que los notarios públicos dan fe de la integridad y contenido que se les presenta.

62. La cuarta hipótesis consiste en la grabación en dispositivos de almacenamiento no modificables, los cuales, por definición, no permiten introducir ningún cambio en un registro una vez que se lo ha almacenado. Esta puede ser una opción práctica y conveniente para las partes interesadas que deseen una alternativa fácilmente disponible y menos costosa.

63. La quinta situación es la de la indagación de los aspectos técnicos dentro de los procedimientos jurídicos, en que el experto designado por el juez puede confirmar la integridad del registro electrónico.

64. La diversidad de situaciones que autorizan la presunción de integridad de un registro electrónico y que se extiende a la presunción de integridad de un ordenador/computador es importante, ya que todas las partes interesadas tendrán acceso a una serie de medios prácticos para generar pruebas electrónicas.

Artículo 8: Versiones impresas

65. La versión impresa de un registro, aunque no sea por sí misma un medio electrónico, está generada por medios electrónicos. Por tanto, si las partes interesadas la han aceptado sistemáticamente como representación verdadera del registro electrónico correspondiente, se puede deducir que es fiable y que cumple con la regla de la mejor prueba. Así lo dispone el Artículo 8, y es importante en la medida en que la mayoría de personas suelen imprimir los registros electrónicos que tienen relación con pruebas por medios electrónicos.

Artículo 9: La carga de probar la autenticidad de la prueba por medios electrónicos

66. Como regla general, en cualquier procedimiento jurídico la persona que desea introducir un registro electrónico como prueba tiene la carga de demostrar su autenticidad.

67. No obstante, las personas más vulnerables, como los consumidores y los niños, pueden verse favorecidos por disposiciones legales que invierten la carga de la prueba. En ese caso, las disposiciones legales prevalecerán sobre la norma general establecida en el Artículo 9.

68. Esta observación es importante debido a que las personas más vulnerables no son por lo general capaces, desde el punto de vista técnico y/o económico, de presentar pruebas basadas en registros electrónicos, pero ello no debe ser obstáculo para que se promueva y garantice su pleno acceso a la justicia y la posibilidad de una defensa adecuada.

Artículo 10: Normas

69. Las prácticas y usos comunes son un indicador importante de lo que podría preverse como pautas de conducta en lo que respecta a la grabación y conservación de registros electrónicos. Por esta razón, la prueba se presentará en base a normas, procedimientos, usos o prácticas actuales, que reflejen esas pautas y den orientación sobre lo que se espera en materia de admisibilidad de los registros electrónicos.

70. En el Artículo 10 se reconoce esa orientación y se establece un nexo con el tipo de negocio o empresa a que se refieren, así como la naturaleza y finalidad del registro electrónico. Esta vinculación es importante, ya que las normas aplicables a un determinado mercado pueden tener objetivos diferentes a las aplicables a otros mercados (por ejemplo, cuando se trata de la seguridad de la información).

71. Este Artículo termina exhortando a las autoridades públicas encargadas de establecer normas técnicas o procedimientos de seguridad a que proporcionen la orientación adecuada para el cumplimiento de sus disposiciones. Ese aspecto es importante, ya que las autoridades competentes pueden y deben proporcionar una orientación general, así como una orientación adaptada a cada mercado o circunstancia, cuando corresponda.

Artículo 11: Declaraciones juradas

72. El Artículo 11 establece que las pruebas por medios electrónicos se pueden presentar en forma de declaraciones juradas. Se trata de otra opción de presentación de pruebas por medios electrónicos que se pone a disposición de los interesados.

73. El grupo de trabajo ha debatido sobre la conveniencia de incluir otras disposiciones en este Artículo para establecer, por ejemplo, que la persona que presta declaración jurada está obligada a hacerlo en la mayor medida de su conocimiento o convicción, y estará sujeta a sanciones impuestas por los tribunales si se determina que dicha declaración fue falsa; otro ejemplo sería una disposición sobre el contrainterrogatorio respecto de las declaraciones juradas.

74. Teniendo en cuenta de que los registros electrónicos son de naturaleza inestable, puede ser preocupante basarse exclusivamente en las declaraciones juradas, y se podría establecer cierto equilibrio haciendo hincapié en la responsabilidad del declarante. Sin embargo, la reglamentación del tema podría solaparse con las normas de procedimiento existentes. Por lo tanto, el grupo de trabajo ha decidido dejar a discreción de los Estados beneficiarios la adopción de este enfoque.

Artículo 12: Acuerdo sobre la admisibilidad de la prueba

75. Como regla general, salvo que una ley disponga otra cosa, las partes en un procedimiento jurídico pueden llegar a un acuerdo sobre la admisibilidad de un registro electrónico, sin perjuicio de lo que decida el tribunal.

76. Esta disposición no se aplicará a los procedimientos penales cuando los acusados no tuvieran asistencia o representación jurídica en el momento de concertación de dicho acuerdo.

77. El Artículo 12 es importante debido a que favorece el acuerdo privado y evita controversias que de otra manera conllevarían costas y demoras innecesarias en los procedimientos judiciales.

Artículo 13: Firma electrónica

78. De manera similar a lo dispuesto en el Artículo 5 con respecto a los registros electrónicos, el Artículo 13 establece en su párrafo 1 que las firmas no serán objeto de discriminación por el mero hecho de estar en formato electrónico.

79. El párrafo 2 se refiere a las diferentes posibilidades para verificar una firma electrónica. Dado el rápido ritmo de los avances tecnológicos en materia de ese tipo de firmas, así como la importancia de ajustarse al principio de neutralidad tecnológica, parece poco probable que puedan delimitarse correctamente las diferentes maneras actuales de comprobar la autenticidad de una firma electrónica.

80. Un ejemplo ilustrativo de la diversidad de maneras de comprobar una firma electrónica se da en el mismo Artículo, cuando se menciona la existencia de un procedimiento mediante el cual una persona debe invocar un símbolo para demostrar que un registro electrónico es suyo (lo que es bastante común en sitios web de Internet para que un usuario pueda entrar en determinadas partes de alguno de esos sitios).

Artículo 14: Requisitos de firma electrónica

81. El párrafo 1 del Artículo 14 establece que las firmas electrónicas cumplen con los requisitos legales como firma de una persona si son suficientemente fiables y adecuadas. Se trata de una disposición importante, pues las firmas electrónicas pueden, en efecto, ser fiables y adecuadas, y algunas veces, incluso más que una firma no electrónica.

82. El párrafo 3 determina que las partes podrán acordar libremente el uso de cualquier método particular de firma electrónica, a menos que la ley disponga otra cosa. Esta disposición es importante porque está en consonancia con los principios generales de libertad de establecimiento de pruebas, al mismo tiempo que ofrece una observación pertinente, por ejemplo, en los casos en que el uso de firmas electrónicas basadas en la criptografía esté en pugna con la vida privada de las personas o las leyes sobre seguridad nacional.

83. Las partes en un acuerdo pueden no especificar el tipo de firma electrónica que utilizarán. Esta situación es bastante común en la práctica, y el párrafo 4 da una solución proporcionando una lista de criterios para cumplir con los requisitos contractuales aplicables a los mensajes de datos con firma electrónica. Entre esos criterios pueden mencionarse la vinculación entre el firmante y los datos de creación de firma (que deberán estar bajo control del firmante), y la posibilidad de detectar cualquier alteración de la firma electrónica en el momento de la firma o ulteriormente.

Artículo 15: Técnicas y procedimientos alternativos para la presentación de pruebas por medios electrónicos

84. El Artículo 15 se refiere a las técnicas y procedimientos alternativos para la presentación de pruebas por medios electrónicos en relación con ciertos registros electrónicos, y destaca i) la certificación por parte de notarios públicos o jueces de paz u otras autoridades competentes, ii) la grabación del registro en un soporte no modificable, y iii) la informática forense en el transcurso de la sustanciación del proceso.

85. Es muy importante que se tenga en cuenta la informática forense, un ámbito de conocimiento especializado en la prueba por medios electrónicos, y en particular, que se haya asociado con la sustanciación del proceso, lo que añade más fiabilidad, ya que se supone que el experto designado por el juez es un profesional imparcial y cualificado.

PARTE III – DISPOSICIONES GENERALES

Artículo 16: Admisibilidad de los registros electrónicos de otros países

86. El Artículo 16 establece la admisibilidad de los documentos electrónicos originados en otra jurisdicción, siempre que se pueda probar o presumir la integridad del ordenador/computador de acuerdo con las mismas normas que se aplican para demostrar la integridad de los registros electrónicos originados en la jurisdicción nacional (es decir, la prueba de que el ordenador funcionaba correctamente y de que el registro electrónico no sufrió ninguna alteración).

87. Esta disposición es importante para la seguridad de las comunicaciones electrónicas con otros países, lo cual a su vez es esencial para los intereses del Estado beneficiario, que desee ampliar las comunicaciones y el comercio electrónicos con otros países.

88. Teniendo en cuenta el hecho de que cada país tiene sus propias reglas sobre la prueba por medios electrónicos, la estipulación de un requisito mínimo, consistente en probar la integridad de los ordenadores/computadores o de los registros electrónicos, puede facilitar la tarea de establecer un denominador común.

Artículo 17: Reconocimiento de firmas y documentos electrónicos extranjeros

89. Mientras que el Artículo 16 trata de los registros electrónicos originados en otros países, el párrafo 2 del Artículo 17 se refiere a la información electrónica ubicada en otros países.

90. Este párrafo enumera una serie de situaciones que pueden determinar que se dé a la información ubicada en una jurisdicción extranjera un trato equivalente a la de la información situada en la jurisdicción nacional. Entre esas situaciones figura la decisión de un tribunal en este sentido y la existencia de un tratado internacional que garantice el correspondiente reconocimiento.

91. Esta disposición es importante porque puede reforzar la seguridad de la corriente de comunicaciones y transacciones electrónicas entre el Estado beneficiario y otros países. Como el acceso a registros electrónicos ubicados en el extranjero para comprobar su integridad puede ser más difícil desde el punto de vista técnico, esta disposición garantiza una serie de procedimientos y situaciones que pueden ayudar a superar esas posibles limitaciones técnicas.

Artículo 18: Interpretación de conformidad con los principios internacionalmente aceptados

92. El Artículo 18 determina que la presente Ley se interpretará y aplicará a la luz de los principios internacionalmente aceptados de neutralidad tecnológica y equivalencia funcional.

93. Estos principios han sido adoptados prácticamente por la totalidad de los países que han reglamentado la prueba por medios electrónicos y los aspectos conexos. El principio de neutralidad tecnológica favorece la inclusión social digital, ya que mejora las posibilidades de desarrollo o uso de tecnologías similares, lo que contribuye a un mayor acceso y precios más bajos. En virtud del principio de equivalencia funcional, no se impondrán en el entorno en línea restricciones que no se apliquen en el universo fuera de línea, lo que tiende a estimular la migración de las comunicaciones y las transacciones hacia la primera opción.

94. Este texto es importante, pues determina que esos principios se aplicarán a cualquier disposición de esta Ley, lo que orientará su interpretación y aplicación hacia los fines sociales y económicos previstos en dichos principios.

Artículo 19: Reglamentos

95. El Artículo 19 faculta al Ministro a emitir reglamentos para dar efecto a los fines de esta Ley y para prescribir todo lo que esta requiera o autorice que se prescriba, y añade que para ello el Ministro puede tener en cuenta las mejores prácticas y normas internacionales.

96. El propósito de este Artículo es reconocer y señalar a la atención la conveniencia de emitir nuevas reglamentaciones para asegurar la correcta aplicación de esta Ley.

97. En este sentido, el grupo de trabajo ha debatido sobre algunos asuntos que se abordarán en los tratados internacionales o en la reglamentación nacional.

98. Se consideró que una serie de cuestiones podrían merecer la atención de los órganos reguladores nacionales, tales como un sistema de acreditación para la firma electrónica (que incluya la autenticación, certificación y acreditación de firmas digitales, atributos y fecha); la integración con las leyes de procedimiento (para garantizar, por ejemplo, que las operaciones de allanamiento e incautación, la orden de presentación, la recopilación de pruebas en tiempo real, el interrogatorio por videoconferencia, los procedimientos jurídicos electrónicos, la preservación inmediata de los datos y la interceptación de las comunicaciones se ajusten a esta Ley); y la integración con las leyes sustantivas relacionadas (sobre retención de datos, responsabilidad de los proveedores de servicios de Internet, y ciberdelincuencia, entre otros ámbitos).

99. Se ha considerado igualmente que algunas tendencias complejas merecían estudios específicos, como la informática en la ''nube de Internet'', la esteganografía (ocultación de la existencia de un mensaje), el *LiveCD* (punto de trabajo autónomo desde un CD) y otras cuestiones que podría generar preocupación de cara a la presentación y reconocimiento de la prueba por medios electrónicos. Es importante llevar a cabo dichos estudios, y crear la correspondiente reglamentación, pues de lo contrario el cumplimiento de las disposiciones de esta Ley podría quedar debilitado u obsoleto.

100. El desarrollo del derecho regional y la armonización con los tratados internacionales se han considerado también temas de interés para el Estado beneficiario, a fin de asegurar una cooperación oficial con otros países y una supervisión y alineación periódicas con las mejores prácticas internacionales vigentes en cada momento. Esta actividad de desarrollo y armonización es importante, pues de lo contrario la aplicación de esta Ley podría tener un alcance limitado o quedar reducida a una cooperación ''extraoficial''.

ANEXOS

Anexo 1:

Participantes en el primer taller de consulta para el Grupo de trabajo del proyecto HIPCAR, sobre el marco legislativo de las TIC – Temas sobre la sociedad de la información Gros Islet, Santa Lucía, 8 a 12 de marzo de 2010

Participantes designados oficialmente y observadores

País	Organización	Apellido	Nombre
Antigua y Barbuda	Ministerio de Información, Radiodifusión, Telecomunicaciones, Ciencia y Tecnología	SAMUEL	Clement
Bahamas	Autoridad Reguladora de los Servicios Públicos y la Competencia	DORSETT	Donavon
Barbados	Ministerio de Finanzas, Inversiones, Telecomunicaciones y Energía	BOURNE	Reginald
Barbados	Ministerio de Industria y Comercio	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministerio de Industria y Comercio	NICHOLLS	Anthony
Belice	Comisión de Servicios Públicos	SMITH	Kingsley
Granada	Comisión Reguladora Nacional de las Telecomunicaciones	FERGUSON	Ruggles
Granada	Comisión Reguladora Nacional de las Telecomunicaciones	ROBERTS	Vincent
Guyana	Comisión de Servicios Públicos	PERSAUD	Vidiahar
Guyana	Oficina del Primer Ministro	RAMOTAR	Alexei
Guyana	Dependencia Nacional de Gestión de Frecuencias	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts y Nevis	Ministerio de Información y Tecnología	BOWRIN	Pierre G.
Saint Kitts y Nevis	Ministerio de la Fiscalía General, Justicia y Asuntos Jurídicos	POWELL WILLIAMS	Tashna
Saint Kitts y Nevis	Ministerio de Promoción de la Juventud, Deportes, Tecnología de la Información, Telecomunicaciones y Correos	WHARTON	Wesley
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	FELICIEN	Barrymore
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	FLOOD	Michael R.
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	JEAN	Allison A.
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	ALEXANDER	K. Andre
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	FRASER	Suenel

Anexo 1

País	Organización	Apellido	Nombre
Suriname	Telecommunicatie Autoriteit Suriname / Autoridad de Telecomunicaciones de Suriname	LETER	Meredith
Suriname	Ministerio de Justicia y Policía, Departamento de Legislación	SITALDIN	Randhir
Trinidad y Tobago	Ministerio de la Administración Pública, División de Servicios Jurídicos	MAHARAJ	Vashti
Trinidad y Tobago	Autoridad de Telecomunicaciones de Trinidad y Tobago	PHILIP	Corinne
Trinidad y Tobago	Ministerio de la Administración Pública, Secretaría de las TIC	SWIFT	Kevon

Participantes de organizaciones regionales/internacionales

Organización	Apellido	Nombre
Secretaría de la Comunidad del Caribe (CARICOM)	JOSEPH	Simone
Comunidad Virtual de las TIC del Caribe (CIVIC)	GEORGE	Gerry
Comunidad Virtual de las TIC del Caribe (CIVIC)	WILLIAMS	Deirdre
Unión de Telecomunicaciones del Caribe (CTU)	WILSON	Selby
Delegación de la Comisión Europea en Barbados y el Caribe Oriental (EC)	HJALMEFJORD	Bo
Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL)	CHARLES	Embert
Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL)	GILCHRIST	John
Autoridad de Telecomunicaciones del Caribe Oriental (ECTEL)	HECTOR	Cheryl
Unión Internacional de Telecomunicaciones (UIT)	CROSS	Philip
Unión Internacional de Telecomunicaciones (UIT)	LUDWIG	Kerstin
Oficina de Negociaciones Comerciales (antes CRNM), Secretaría de la Comunidad del Caribe (CARICOM)	BROWNE	Derek E.
Secretaría de la Organización de Estados del Caribe Oriental (OECS)	FRANCIS	Karlene

Consultores del HIPCAR participantes en el taller

Apellido	Nombre
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[7]	J Paul
PRESCOD	Kwesi

[7] Presidente del taller.

Anexo 2:

Participantes en el segundo taller de consulta (Fase B) del Grupo de trabajo del proyecto HIPCAR, sobre el marco legislativo de las TIC – Temas sobre la sociedad de la información
Crane, St. Philip, Barbados, 23 a 26 de agosto de 2010

Participantes designados oficialmente y observadores

País	Organización	Apellido	Nombre
Antigua y Barbuda	Ministerio de Información, Radiodifusión, Telecomunicaciones, Ciencia y Tecnología	SAMUEL	Clement
Bahamas	Autoridad Reguladora de los Servicios Públicos y la Competencia y	DORSETT	Donavon
Barbados	Ministerio de Asuntos Económicos, Empoderamiento, Innovación y Comercio	NICHOLLS	Anthony
Barbados	Ministerio de Finanzas, Inversiones, Telecomunicaciones y Energía	BOURNE	Reginald
Barbados	Ministerio de la Administración Pública	STRAUGHN	Haseley
Barbados	University of the West Indies	GITTENS	Curtis
Belice	Comisión de Servicios Públicos	PEYREFITTE	Michael
Dominica	Gobierno de Dominica	ADRIEN-ROBERTS	Wynante
Dominica	Ministerio de Información, Telecomunicaciones y Fomento de la Ciudadanía	CADETTE	Sylvester
Dominica	Ministerio de Turismo y Asuntos Jurídicos	RICHARDS-XAVIER	Pearl
Granada	Comisión Reguladora Nacional de las Telecomunicaciones	FERGUSON	Ruggles
Guyana	Oficina del Presidente	RAGHUBIR	Gita
Guyana	Comisión de Servicios Públicos	PERSAUD	Vidiahar
Jamaica	Fiscalía General del Estado	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Grupo Digicel	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Jamaica	Ministerio de Seguridad Nacional	BEAUMONT	Mitsy
Jamaica	Oficina del Primer Ministro	MURRAY	Wahkeen
Saint Kitts y Nevis	Fiscalía General del Estado	POWELL WILLIAMS	Tashna
Saint Kitts y Nevis	Departamento de Tecnología, Centro Nacional de TIC	HERBERT	Christopher
Saint Kitts y Nevis	Ministerio de Promoción de la Juventud, Deportes, Tecnología de la Información, Telecomunicaciones y Correos	WHARTON	Wesley
Santa Lucía	Fiscalía General del Estado	VIDAL-JULES	Gillian
Santa Lucía	Ministerio de Comunicaciones, Obras Públicas, Transporte y Servicios Públicos	FELICIEN	Barrymore
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	ALEXANDER	Kelroy Andre

Anexo 2

País	Organización	Apellido	Nombre
San Vicente y las Granadinas	Ministerio de Telecomunicaciones, Ciencia, Tecnología e Industria	FRASER	Suenel
Suriname	Ministerio de Comercio e Industria	SAN A JONG	Imro
Suriname	Ministerio de Transportes, Comunicaciones y Turismo	STARKE	Cynthia
Suriname	Telecommunicatie Autoriteit Suriname / Autoridad de Telecomunicaciones de Suriname	PELSWIJK	Wilgo
Suriname	Telecommunicatiebedrijf Suriname / Telesur	JEFFREY	Joan
Trinidad y Tobago	Ministerio de Seguridad Nacional	GOMEZ	Marissa
Trinidad y Tobago	Ministerio de la Administración Pública, Secretaría de las TIC	SWIFT	Kevon
Trinidad y Tobago	Ministerio de la Administración Pública, Departamento de Servicios Jurídicos	MAHARAJ	Vashti
Trinidad y Tobago	Ministerio de la Fiscalía General, Fiscalía General	EVERSLEY	Ida
Trinidad y Tobago	Autoridad de Telecomunicaciones de Trinidad y Tobago	PERSAUD	Karina
Trinidad y Tobago	Telecommunications Services Limited de Trinidad y Tobago	BUNSEE	Frank

Participantes de organizaciones regionales/internacionales

Organización	Apellido	Nombre
Centro del Caribe de Administración del Desarrollo (CARICAD)	GRIFFITH	Andre
Secretaría de la Comunidad del Caribe (CARICOM)	JOSEPH	Simone
Comunidad Virtual de las TIC del Caribe (CIVIC)	HOPE	Hallam
Comunidad Virtual de las TIC del Caribe (CIVIC)	ONU	Telojo
Unión de Telecomunicaciones del Caribe (CTU)	WILSON	Selby
Telecomunicaciones del Este del Caribe (ECTEL)	WRIGHT	Ro Ann
Unión Internacional de Telecomunicaciones (UIT)	CROSS	Philip
Unión Internacional de Telecomunicaciones (UIT)	LUDWIG	Kerstin
Secretaría de la Organización de Estados del Caribe Oriental (OECS)	FRANCIS	Karlene

Consultores del HIPCAR participantes en el Taller

Apellido	Nombre
ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[8]	J Paul
PRESCOD	Kwesi

[8] Presidente del taller.

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Place des Nations
CH-1211 Ginebra

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Ginebra, 2013