ECONOMÍA DIGITAL

GUÍA DE UN ENTORNO PROPICIO

ÁREAS CLAVE DE DIÁLOGO PARA EMPRESAS Y RESPONSABLES DE FORMULAR POLÍTICAS

Esta publicación fue parcialmente financiada por National Endowment for Democracy

El **Centro para la Empresa Privada Internacional (CIPE, por sus siglas en inglés)** fortalece la democracia en todo el mundo a través de la empresa privada y reforma orientada al mercado para expandir el acceso a oportunidades para todos los ciudadanos y crear una democracia efectiva. Al mejorar el clima de los negocios para los empresarios y derribar las barreras legales y regulatorias a través de una defensa de políticas, incluso el uso de tecnología, el CIPE ha apoyado al sector privado para que sea la fuerza motriz de la reforma. Al trabajar con organizaciones del sector privado a nivel mundial, el CIPE ayuda a los negocios a expresarse en la formulación de políticas en una variedad de cuestiones de economía digital, incluso internet abierta. **www.cipe.org.** El CIPE es un instituto central de la Centro para la Empresa Privada Internacional y una afiliada de la Cámara de Comercio de los EE. UU.

New Markets Lab (NML, por sus siglas en inglés) es un centro sin fines de lucro de derecho, desarrollo e iniciativa empresarial que cuenta con experiencia comparativa y un equipo internacional de abogados enfocados en la reforma económica legal y regulatoria socialmente responsable. NML considera el derecho como una fuerza motriz que puede generar iniciativa empresarial y desarrollo económico. Las leyes y regulaciones económicas deben ser claras y accesibles, particularmente si las pequeñas empresas, las mujeres y los pobres se beneficiarán del crecimiento económico. Sin normas que estén mejor diseñadas y aplicadas y abogados capacitados que puedan resolver problemas de una manera nueva, la mayoría de los mercados tienden a estar abiertos solo para aquellos con los recursos para afectar la toma de decisiones. La organización ha desarrollado un enfoque único y ha establecido un conjunto de herramientas legales que dan a aquellos con desventaja económica un rol más directo para conformar sistemas regulatorios y proporcionar capacitación práctica para los jóvenes abogados de países en desarrollo y países desarrollados por igual. **www.newmarketslab.org**

Descargo de responsabilidad: Esta publicación del Centro para la Empresa Privada Internacional (CIPE) y New Markets Lab (NML) brinda información general en relación con la política actual y los entornos regulatorios en la economía digital basada en la investigación. La publicación pretende ser para fines informativos únicamente. Esta publicación no brinda asesoramiento legal de ningún tipo y no se debe utilizar como reemplazo a obtener asesoramiento legal. Si bien el CIPE y NML han realizado grandes esfuerzos para asegurar que la información en esta guía sea precisa, ninguna de las organizaciones puede garantizar que la información sea completa o actualizada. El CIPE y NML recomiendan fervientemente que los lectores consulten a un abogado con licencia si requieren asesoramiento legal.

Reconocimientos

Editora

LOUISA TOMAR, Responsable de Programas Globales, CIPE

Autores principales

KATRIN KULHMANN, Presidente y Fundadora, New Markets Lab

MENGYI WANG, Especialista Legal Internacional, New Markets Lab

MEGAN GLAUB, Investigadora Legal Sénior, New Markets Lab

ANA MARÍA GARCÉS ESCOBAR, Investigadora Legal, New Markets La

Colaboradores

KIM ERIC BETTCHER, Ph.D., Directora de Gestión del Conocimiento, CIPE

ANNA KOMPANEK, Directora de Programas Globales, CIPE

LOUISA TOMAR, Responsable de Programas Globales, CIPE

MORGAN FROST, Asistente del Responsable de Programas Globales, CIPE

ADITI RAO, Investigador Legal, New Markets Lab

LANXIN CHEN, Pasante Legal, New Markets Lab

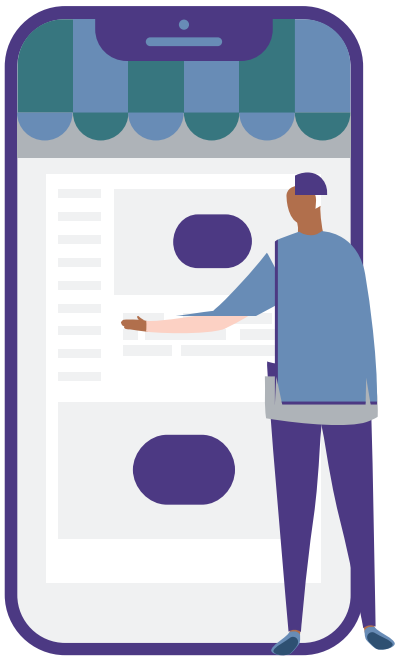
Un agradecimiento especial a
Brian Bieron, Director Ejecutivo, eBay Inc. Public Policy Lab
y Miembro del Directorio del Centro para la Empresa Privada Internacional.

Tabla de contenidos

Parte I – Guía Resumida de la economía digital

Introducción

La economía digital en expansión, que incluye servicios transfronterizos y comercio electrónico (e-commerce), puede ser un impulsor importante del desarrollo democrático y económico porque abre nuevos canales de mercado para empresas locales, promoviendo el comercio inclusivo e impulsando ingresos fiscales para los gobiernos para aumentar el acceso a los servicios esenciales. A medida que la innovación se extiende por todo el mundo, las comunidades empresariales locales, particularmente en el Hemisferio Sur, continúan enfrentando barreras para superar las divisiones tecnológicas y digitales. Las políticas, leyes y regulaciones nacionales que rigen este nuevo espacio influyen considerablemente los resultados de desarrollo. Los negocios y organizaciones locales que las representan deben estar equipados para defender un entorno propicio que promueva el crecimiento inclusivo en un futuro digital.



Para ese fin, el Centro para la Empresa Privada Internacional (CIPE) y New Markets Lab (NML) se unieron para elaborar esta Guía que pretende apoyar los diálogos de política sobre temas cruciales para fortalecer los entornos comerciales digitales inclusivos en todo el mundo.

En la actualidad, no hay un consenso con respecto a un conjunto de normas y estándares globales armonizados para guiar y alinear el cambio regulatorio para la economía digital. Por lo tanto, es esencial que las comunidades empresariales locales y los reformistas con ideas similares entiendan y aborden los complejos sistemas digitales que evolucionan en el nivel internacional, regional, nacional y, a veces, subnacional. La economía global continúa cambiando al ámbito digital, mientras que las normas y regulaciones que permiten la economía digital aún se encuentran en etapas iniciales en muchos países y, a menudo, impiden el crecimiento local y el acceso a los mercados mundiales. Al mismo tiempo, la innovación tecnológica y los riesgos cibernéticos están superando el desarrollo de estrategias nacionales y requieren cada vez más enfoques novedosos y mayor cooperación internacional.

Como la actividad económica se produce cada vez con más frecuencia en línea, las comunidades empresariales locales deben tener voz con respecto a cómo las normas y regulaciones para el comercio electrónico y el comercio digital se diseñan y se implementan para asegurar su participación y sostenibilidad en línea y fuera de línea. Muy a menudo, los marcos que rigen la economía digital son impulsados por los gobiernos, con una participación mínima de las partes

interesadas, como las pequeñas y medianas empresas, cuyas voces son esenciales para el desarrollo económico inclusivo. Al mismo tiempo, muchos gobiernos buscan alcanzar los Objetivos de Desarrollo Sostenible (SDG, por sus siglas en inglés) de las Naciones Unidades a través de iniciativas enfocadas en tecnología y asociaciones como la Visión 2030[1], una plataforma establecida por el Pacto Global de las Naciones Unidas, el Consejo Británico y otros para el diálogo y colaboración a fin de entender el potencial de lo digital para alcanzar los SDG y explorar el rol que el sector de la tecnología puede tener para apoyar los esfuerzos de las industrias. Nunca hubo un mejor momento para que las comunidades empresariales locales se unan a este diálogo democrático para asegurar que se aborden sus necesidades e inquietudes.

Esta Guía pretende explicar los complejos aspectos legales y regulatorios de la economía digital para todas las partes interesadas, sin importar su conocimiento técnico o experiencia en política. Se divide

- **Parte uno: Guía Resumida de la economía digital** comienza con una definición de la economía digital e identifica las diferentes audiencias de la Guía, que incluyen comunidades empresariales locales, organismos reguladores y la sociedad civil. Ofrece información sobre cómo aprovechar la Guía y las vías para la defensa y el diálogo. Los cuatro temas principales que se cubren – **protección del consumidor, protección de datos, ciberseguridad y transacciones electrónicas (pagos electrónicos y firmas electrónicas)** – se seleccionaron a través de una evaluación y debates continuos con socios del CIPE en mercados emergentes y fronterizos. Los cuatro temas se definen y se debaten en el contexto de la defensa empresarial y cada sección contiene una lista de verificación para evaluar los marcos legales y regulatorios nacionales existentes. La Guía Resumida concluye con información sobre la metodología desarrollada por NML y un llamado a la acción para un diálogo democrático.

- **Parte dos: El Análisis Profundo Legal** incluye información más detallada sobre los **marcos internacionales y regionales** aplicables a cada uno de los cuatro temas de economía digital; ejemplos de diferentes **enfoques regulatorios** que se utilizan en todo el mundo; consideraciones para la **implementación y aplicación** de leyes y regulaciones; y los **marcos institucionales** que existen para cada uno.

1. *2030 Vision – Technology Partnerships for the Global Goals, https://www.2030vision.com/get-involved/2030vision-uniting-to-deliver-technology-for-the-global-goals2. International Monetary Fund, Measuring the Digital Economy. pág. 6. Web. 5 de abril de 2018*

La economía digital

¿Qué significa exactamente "economía digital"? Esta Guía adopta una definición amplia: la digitalización de la actividad económica que incorpora datos e internet "en productos y procesos de producción, nuevas formas de consumo doméstico y gubernamental, formación de capital fijo, flujos transfronterizos y finanzas[2].

La economía digital se ha convertido en un elemento predominante de la vida diaria en la mayoría de los países. La rápida difusión de internet ha cambiado cómo los negocios operan y hacen transacciones con los consumidores, cómo los ciudadanos obtienen servicios públicos y cómo los organismos reguladores trabajan en el nivel local e internacional. La digitalización hace surgir nuevos modelos de negocios, nuevas cadenas de suministro transfronterizos, y nuevos riesgos. Bienes y servicios que se comercializan en línea, el contenido digital y el análisis de datos se están convirtiendo rápidamente en productos que se comercializan globalmente.

Como internet, la economía digital es verdaderamente global; no tiene fronteras, y las personas que se pueden conectar pueden acceder de inmediato a los mercados en todo el mundo. La naturaleza de esta economía da a lugar preguntas únicas con respecto a cómo regularla. Los enfoques tradicionales para proteger a los consumidores, cumplir con contratos y almacenar información deben ser reevaluados para el ámbito digital. Además, las leyes, regulaciones y políticas que rigen la economía digital deben trabajar en consistencia con los esfuerzos para impulsar el entorno operacional, incluso infraestructura de IT, servicios, plataformas, ecosistemas y dispositivos. Por ejemplo, electricidad confiable, redes de telecomunicaciones y fibra óptica son infraestructuras críticas que se deben abordar junto con las cuestiones legales y regulatorias.

Si bien muchos factores afectan la economía digital, esta Guía se enfoca en cuatro áreas principales: (1) **protección del consumidor**, (2) **protección de datos**, (3) **ciberseguridad**, y (4) **transacciones electrónicas, específicamente pagos electrónicos (e-payments)** y **firmas electrónicas (e-signatures)**. Juntos, estos temas constituyen una gran parte del entorno propicio para la economía digital y afectan a casi todos los aspectos de cómo se realizan los negocios en línea de manera responsable y segura. De forma individual y conjunta, estas cuestiones pueden actuar como multiplicadores de la fuerza para una reforma más amplia y son fundamentales para las oportunidades comerciales y las preocupaciones del gobierno.

2. *International Monetary Fund, Measuring the Digital Economy. pág. 6. Web. 5 de abril de 2018*

¿Esta guía es para mí?

La Guía se enfoca en las cuatro áreas principales que se enumeran arriba desde la perspectiva de las **comunidades empresariales locales**, incluso **empresarios** y **pequeñas y medianas empresas** (PyMEs). Apunta a proporcionar la información más fundamental necesaria para entender el panorama de política actual, mejorar el cumplimiento de las normas y detectar problemas para el diálogo continuo y reforma. Si bien no es prescriptivo, trata sobre cómo identificar las oportunidades de defensa y diálogo con responsables de formular políticas para desarrollar una economía digital inclusiva.

Esta Guía también está diseñada para proporcionar a la comunidad empresarial local, incluso **asociaciones empresariales**, **cámaras de comercio** y **grupos de expertos económicos** (especialmente en mercados emergentes y fronterizos) un marco para entender los conceptos principales que componen el entorno legal y regulatorio en torno a la economía digital.

Además, este recurso pretende complementar el conocimiento necesario que necesitan las **responsables de formular políticas** y **organismos reguladores** para desarrollar e implementar políticas y regulaciones eficaces. El Análisis Profundo Legal cubre cada uno de estos cuatro temas de enfoque haciendo un análisis profundo de las consideraciones regulatorias y los marcos internacionales existentes.

Todas las partes interesadas, incluso las **organizaciones internacionales** y **de sociedad civil**[3] pueden usar esta herramienta para ayudar a identificar los puntos de intervención clave y las oportunidades para involucrar a las empresas locales y al gobierno en el diálogo. La Guía aborda las normas existentes en torno a la economía digital, brinda una base para la defensa de políticas basada en las buenas prácticas proporciona un lenguaje compartido para el muy necesario diálogo entre múltiples interesados.

3. *Resulta útil aquí indicar brevemente la diferencia entre leyes, regulaciones y política. Las leyes, que generalmente deben atravesar un proceso parlamentario, crean un marco para regir el mercado y, a menudo, se relacionan con un determinado sector o actividad. Las leyes tienden a ser más generales y crean obligaciones legalmente aplicables. Las regulaciones se crean, generalmente a través de acciones, para implementar leyes y tienden ser más detalladas y también más fáciles de cambiar. Las políticas, que son la categoría más amplia de medidas, brindan orientación a las partes interesadas y funcionarios de gobierno con respecto a qué objetivos las leyes y regulaciones deben buscar alcanzar, pero no tienden a ser instrumentos legalmente vinculantes por sí mismos.*

Aprovechar la guía

La tecnología cambia tan rápidamente que sin un mecanismo apropiado, la participación del sector público-privado en temas de economía digital nunca podrá mantenerse al día. Dependiendo de las circunstancias locales, las prioridades de política pública pueden ser nuevas leyes y regulaciones, o una mejor implementación de las normas existentes. En todos los casos, el diálogo democrático requiere que las partes interesadas lleven mensajes bien preparados a las discusiones sobre políticas.

La preparación implica comprender y priorizar los temas de alto nivel que se describen en esta Guía, sopesar las posiciones que las empresas pueden tomar, mapear a las partes interesadas con ideas afines y aclarar los resultados deseados. Al articular cuestiones de prioridad y resultados concretos, las comunidades empresariales locales pueden ir más allá de una lista de preguntas amplias para enfocarse en intervenciones que podrían influir en cómo la economía digital se define a nivel local y global. Desarrollar conocimiento sobre los temas clave también puede proporcionar una base para un amplio rango de partes interesadas para que intercambien opiniones sobre los objetivos y las prioridades de políticas, haciendo hincapié en que el diálogo inclusivo no solo satisface los intereses particulares, sino también apoya objetivos de desarrollo social y económico más amplios.

Defensa de políticas y diálogo

¿Qué es defensa?

La economía digital es un área de prioridad para que las empresas locales se involucren con organizaciones empresariales como cámaras de comercio, asociaciones empresariales y grupos expertos económicos que pueden ser conductos valiosos para la defensa de políticas. La defensa es un esfuerzo de influir e involucrarse en una política pública de manera abierta y transparente. Como herramienta de sociedad civil, aborda cuestiones de mucha preocupación para la comunidad y aboga por el cambio presentando evidencia y apoyo de grupos de electores cívicos. La defensa apoya la toma de decisiones y a la vez informa y empodera al público. A través de la defensa, el sector privado comparte información y perspectivas profesionales esenciales con el gobierno sobre mercados y el entorno operativo empresarial. El gobierno se beneficia de esta información de nivel de base en la economía para entender los efectos de sus decisiones políticas.

¿Qué es el diálogo público-privado?

El diálogo público-privado (PPD, por sus siglas en inglés) es un enfoque estructurado, participativo e inclusivo para la formulación de políticas. El diálogo mejora el flujo de la información en relación con la política económica, en este caso la economía digital, y desarrolla legitimidad en el proceso de políticas. También busca superar impedimentos para la transparencia y lograr una mayor inclusión de partes interesadas en la toma de decisiones.

Si bien las características técnicas y regulatorias de la economía digital que se analizan en toda esta Guía pueden ser nuevas para muchas responsables de formular políticas y grupos de defensa empresarial, el Centro para la Empresa Privada Internacional (CIPE) cuenta con décadas de experiencia apoyando a reformistas locales y la participación del sector privado en un diálogo democrático y esfuerzos de reforma política pública.

Preguntas de defensa para guiar la estrategia

- **¿Qué se debe cambiar?**
- **¿Quién puede hacer los cambios?**
- **¿Cuánto cambio se debe hacer?**
- **¿Cuándo se deben hacer los cambios?**
- **¿Cómo se pueden exponer los argumentos para el cambio?**
- **¿Cómo se implementarán los cambios?**

Fuente: CIPE, How to Advocate Effectively: A Guidebook for Business Associations

En los últimos 35 años, el CIPE ha apoyado a más de 1,000 iniciativas locales en más de 100 países en desarrollo, y ha creado numerosos recursos disponibles públicamente, incluso la Agenda Empresarial Nacional (NBA, por sus siglas en inglés)[4] y un kit de herramientas de PPD para asistir con los esfuerzos participativos de elaboración de políticas en todo el mundo. Esta Guía sirve como herramienta para enfocar el proceso de defensa y como recurso regulatorio y legal para que las contrapartes del sector público y privado desarrollen un lenguaje compartido para las etapas iniciales del diálogo.

La clave para iniciar un diálogo productivo es encontrar un tema que genere controversia, un tema de gran interés actual que promueva la acción y abra la puerta para abordar áreas relacionadas de importancia estratégica[5]. Un ejemplo de un tema que genera controversia en la economía digital puede ser desde una preocupación por un nuevo requisito de localización de datos problemático hasta la necesidad de una implementación más generalizada de una ley de firma electrónica que se aprobó recientemente en el parlamento. La preparación para un diálogo más serio lleva meses, durante los cuales la comunidad debe evaluar los desafíos y opciones de políticas, movilizar a las partes interesadas y formular posiciones.

Las cámaras de comercio y las asociaciones empresariales requieren métodos para recolectar y procesar información de la comunidad empresarial sobre sus necesidades y objetivos. Estos pueden diferir considerablemente dependiendo de si una empresa provee bienes o servicios en línea o ninguno de los dos. Se puede recopilar información de múltiples maneras, incluso encuestas, grupos de enfoque y extensión a miembros de la asociación y coalición. Es necesario recopilar información sobre los muchos desafíos que enfrentan las empresas locales – no solo multinacionales o compañías de tecnología – e identificar las posibles soluciones. Lograr un consenso sobre las posiciones de política puede ser difícil porque los empresarios pueden tener diferentes intereses en la economía digital. La clave es equilibrar las demandas competitivas y priorizar los objetivos compartidos.

Las organizaciones comerciales que se embarcan en esfuerzos de defensa también deben involucrar a la comunidad empresarial

4. *CIPE. National Business Agenda Guidebook. Web. 2006.*
5. *Bettcher, Kim E. (CIPE) Making the Most of Public-Private Dialogue: An Advocacy Approach. Web. 2011.*

más amplia y la sociedad civil para adquirir un entendimiento mutuo y aliados. Las coaliciones, basadas en un interés común – por ejemplo, expandir el acceso al comercio electrónico para las PyMEs locales – pueden incorporar diferentes grupos de partidarios dependiendo de la cuestión. Ya sea que las coaliciones son temporarias o permanentes, todos los miembros deben presentar un mensaje común para influir de manera creíble la política pública. Cuando se forman coaliciones para crear una economía digital más inclusiva, es importante considerar aliados como nuevas empresas, organizaciones de sociedad civil, defensores de internet abierta, compañías de tecnología y organizaciones multilaterales como la Comisión de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, por sus siglas en inglés).

El diálogo siempre está seguido por pasos de implementación y monitoreo de política. Esto incluye una presión para el seguimiento por parte del sector privado y otros partidarios. Es importante que la comunidad empresarial considere el ritmo del cambio tecnológico cuando evalúa los resultados deseados de política; la velocidad de la innovación necesita un análisis continuo de la efectividad de las leyes y regulaciones vigentes.

Para mantener una amplia coalición de reformistas comprometidos, debe haber un medio de informar a los electores sobre los resultados del diálogo y educar a la comunidad sobre las nuevas políticas y normas. La reforma requiere un esfuerzo continuo que se basa en logros anteriores. Después de cada fase de diálogo, es importante evaluar las lecciones y las oportunidades que emergieron, refinar las estrategias de defensa, y prepararse para la siguiente fase. Con el tiempo, estos esfuerzos pueden promover una economía digital y democracia más inclusiva.

3 claves para la defensa exitosa:

1. **INTERÉS DE LOS ELECTORES: consultar y escuchar a los miembros de asociaciones y coaliciones antes de establecer el tema (o temas) de defensa objetivo.**

2. **BENEFICIO MÁS AMPLIO: evitar cuestiones que afectan a intereses limitados y dé prioridad a las cuestiones que afectan a múltiples sectores de la economía.**

3. **VIABILIDAD: concentrar los esfuerzos de defensa en áreas de política donde hay una buena posibilidad de lograr resultados positivos o, al menos, mitigar el impacto negativo.**

Lista de verificación para representación de las partes interesadas en el proceso de defensa de políticas[6]

- [ ] Encuestar a los miembros o coalición sobre las cuestiones de la economía digital más importantes o urgentes
- [ ] Determinar y analizar las leyes y regulaciones vigentes que aplican a las cuestiones de prioridad
- [ ] Definir la posición oficial de los miembros o coalición sobre la base de la evidencia y análisis
- [ ] Identificar a los responsables de la toma de decisiones e influyentes (sector de la industria, ministerio de gobierno/organismo regulatorio, etc.)
- [ ] Determinar el mejor método de comunicación para contactar a los responsables de la toma de decisiones e influyentes
- [ ] Preparar materiales de comunicación y mensajes (radio, redes sociales, etc.) apoyados por investigación y hechos
- [ ] Implementar la campaña de defensa y hacer un seguimiento del progreso y los logros
- [ ] Evaluar la efectividad de la campaña y evaluar la implementación del cambio de políticas o cambio regulatorio

6. *Para más información sobre la defensa, visite: https://www.cipe.org/vba/business-associations-guidebook/*

   https://www.cipe.org/legacy/publication-docs/advocacyguidebook_english.pdf

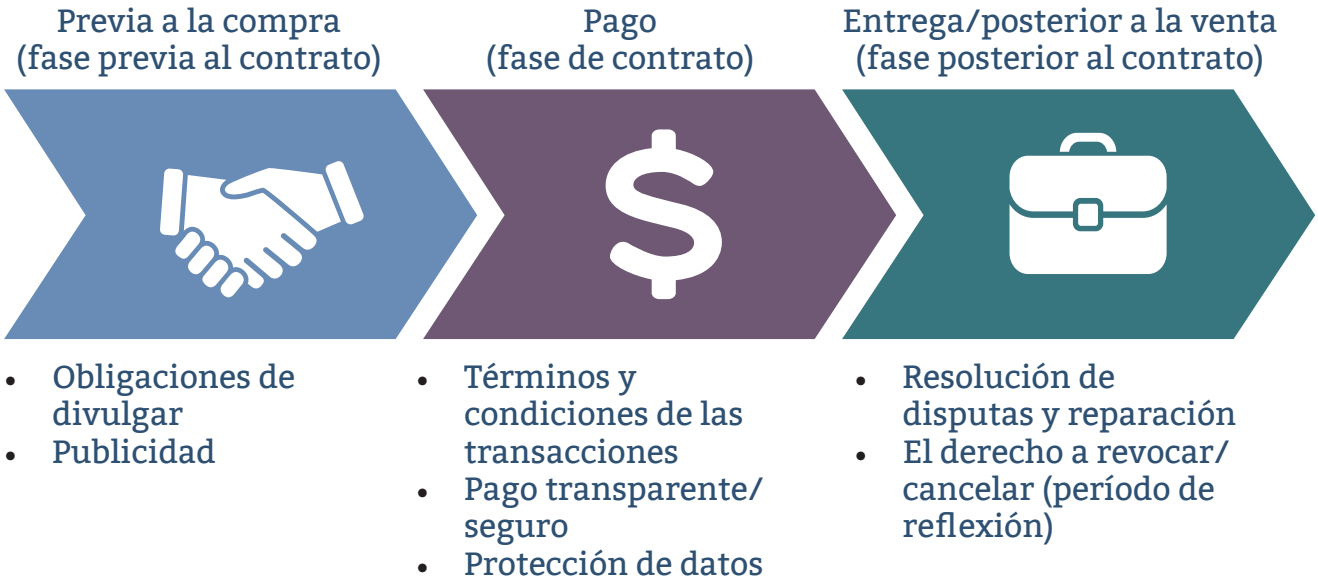
Entender el problema – Protección del consumidor

La protección del consumidor es una área importante de la ley que protege a las personas y empresas que compran bienes y servicios a través de medios electrónicos y no electrónicos. Las leyes de protección del consumidor buscan proteger a los consumidores de "bienes y servicios descritos incorrectamente, dañados, fallados y peligrosos, y de prácticas comerciales y crediticias injustas."[7]

La protección del consumidor en el comercio electrónico es esencial para promover un entorno confiable en línea. Tener un régimen de protección del consumidor fuerte también beneficiaría a la comunidad empresarial local – por ejemplo, a través de transacciones de empresa a empresa (B2B) – mejorando la confianza en el comercio electrónico, simplificando las transacciones digitales y expandiendo la base del consumidor. Crear un entendimiento de base de los derechos y obligaciones para proteger a los consumidores en línea ayudará a las empresas locales y grupos de defensa a participar en un diálogo continuo de política en esta área emergente.

En la actualidad, los regímenes convencionales de protección del consumidor, en general, no están diseñados para abordar nuevas prácticas, como la publicidad en redes sociales. Como resultado, muchos gobiernos no tienen las protecciones adecuadas. La regulación de la protección del consumidor en el comercio electrónico se enfoca en preguntas clave: (1) **cómo equilibrar los derechos y obligaciones entre las partes interesadas** (gobiernos, industria y consumidores) y (2) **cómo integrar consideraciones específicas del comercio electrónico en regímenes convencionales de protección del consumidor**. Las regulaciones tienden a relacionarse con tres etapas principales de transacciones del consumidor: la fase previa a la compra (obligaciones de divulgar y publicidad), la fase de pago (términos y condiciones de las transacciones, pago transparente/seguro y

Diagrama 1. Elementos regulatorios de la protección del consumidor



Fuente: New Markets Lab (2018)

7. *Your Dictionary, Consumer Protection Law – Legal Definition. Web.*

protección de datos) y la fase de entrega/posterior a la venta (resolución de disputas y reparación y el derecho a revocar/cancelar o período de reflexión). (Consulte **Diagrama 1**).

Una parte particularmente importante de la protección del consumidor es la resolución de disputas. La resolución de disputas es esencial para empresas y para consumidores por igual, ya que las disputas entre comerciantes y clientes surgen con frecuencia en transacciones electrónicas en la fase posterior a la venta). Las PyMEs en los mercados en desarrollo con frecuencia citan el cumplimiento con las leyes de protección del consumidor y consideran las medidas relevantes de resolución de disputas un desafío para desarrollar su presencia digital[8]. Un obstáculo importante es la aplicación de las leyes y regulaciones que ya podrían existir. Este fue el caso en Perú (consulte el estudio de caso a continuación). Para agilizar la aplicación, los gobiernos y empresas están recurriendo cada vez más a medios alternativos de resolución de disputas, especialmente la resolución de disputas en línea (ODR, por sus siglas en inglés). Por ejemplo, tanto México como Brasil han implementado mecanismos de ODR respaldados por el gobierno. En el sector privado, las empresas como eBay, Alibaba y PayPal tienen versiones de ODR.

A pesar de la importancia de contar con regímenes de protección del consumidor claros tanto para las empresas como para los consumidores, la protección del consumidor es a menudo una de las últimas áreas en las que las economías en desarrollo se enfocan y regulan a medida que crean marcos en torno al comercio electrónico. A nivel internacional, la protección del consumidor tampoco ha recibido la atención que merece, y hay poco consenso sobre los estándares. Las leyes y regulaciones claras y bien aplicadas son importantes para que las compañías puedan desarrollar confianza con los consumidores; especialmente en economías predominantemente basadas en efectivo donde la confianza en general se desarrolla cara a cara. Debido a la naturaleza global de la economía digital, la comparabilidad entre los marcos legales y regulatorios nacionales aliviaría la carga para las empresas y los organismos reguladores. La armonización global en torno a los elementos de protección del consumidor ayudaría a crear expectativas estándar entre los consumidores y normas comunes para los comerciantes, creando una mayor seguridad legal y confianza en general.

8. *International Trade Centre, New Pathways to E-Commerce; a Global MSME Competitiveness Survey. Web. 25 de septiembre de 2017*

Estudio de caso:
Resolución de disputas en línea en Perú

Si bien una jurisdicción puede tener un conjunto de leyes sólido y exhaustivo en relación con la protección del consumidor y aplicación de contratos, sin instituciones legales igualmente sólidas, ni los consumidores ni la comunidad empresarial tendrán la confianza para realizar transacciones. Este fue caso en Perú, donde un sistema judicial ineficiente dificultó aplicar las regulaciones de protección del consumidor, con un impacto negativo para el comercio y las inversiones en general. Una asociación entre el banco estatal de desarrollo Corporación Financiera de Desarrollo (COFIDE) y la organización sin fines de lucro Innovations for Poverty Action (IPA) ayudó a mejorar la situación.

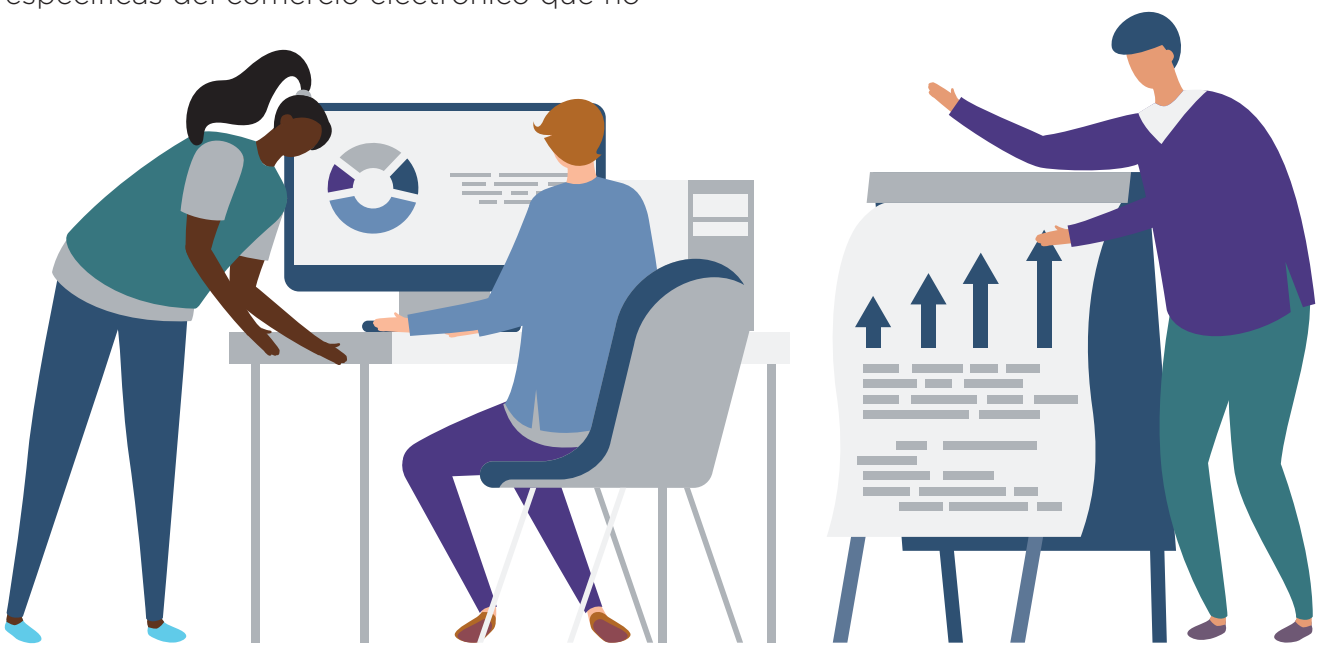
COFIDE e IPA colaboraron para crear una plataforma piloto de resolución de disputas en línea que incorpora información enfocada en el usuario como un mecanismo de sanción, evaluaciones y clasificaciones para mejorar la aplicación de contratos en el distrito de Gamarra de Lima, donde se encuentra el más grande grupo de prendas de Latinoamérica. El sistema de ODR ha sido especialmente útil debido a la economía de Perú que – si bien es una de las más rápido crecimiento en Latinoamérica – aún es pequeña y muy informal. Las comunidades empresariales que enfrenta problemas similares podrían copiar este enfoque asociándose con organizaciones de sociedad civil y el sector público con el objetivo de fortalecer la seguridad del consumidor y la confianza en el sistema judicial progresivamente y a la vez proporcionar un modelo para reforma del estado de derecho más institucionalizada.

Fuente: FHI360, The Atlas of innovation for Economic Stability, Web, mayo de 2018.

Guía para empresas y recomendaciones

Para entender mejor sus obligaciones legales, las empresas locales primero deben entender dónde residen las responsabilidades de protección del consumidor. La responsabilidad tiende a asignarse en la industria (particularmente plataformas de comercio electrónico y proveedores en línea), organismos reguladores y consumidores. Cada etapa de una transacción – previa a la compra, pago y posterior a la venta/entrega – tiene consideraciones regulatorios con diferentes responsabilidades. Entender las reglas en cada etapa de la transacción y realizar autorregulación podría mejorar la calidad de la marca e incrementar aún más la posibilidad de participación del consumidor, minimizando el riesgo y las consecuencias para la reputación en el caso de una disputa. La comunidad empresarial también debe analizar si hay actividades comerciales específicas del comercio electrónico que no están cubiertas por un régimen regulatorio existente (por ejemplo, publicidad en las redes sociales) y considerar si estas actividades deberían incluirse en un enfoque de defensa.

Existen iniciativas para abordar la protección del consumidor en un mercado global, pero tienden a ser de naturaleza general y no brindan suficiente orientación a empresas, gobiernos o consumidores. Los grupos de defensa empresarial que buscan participar en esta área podrían trabajar con las responsables de formular políticas y otros defensores para crear iniciativas, disposiciones y medidas específicas que se ajusten a las necesidades de los consumidores (por ej., protección contra falsificaciones o bienes fraudulentos) y empresas (por ej., protección de la propiedad intelectual o violación de la marca registrada).



A medida que la comunidad empresarial local explora el panorama legal y regulatorio para la protección del consumidor, cuatro consideraciones regulatorias principales podrían ayudar a estructurar los modelos empresariales e informar los esfuerzos de defensa.

Son 1) **grado de responsabilidad empresarial por las plataformas de comercio electrónico**, 2) **resolución de disputas,** 3) **un derecho establecido a revocar/período de reflexión**, y 4) **estructuras institucionales para regular la protección del consumidor en el comercio electrónico.**

- **Grados de responsabilidad empresarial:** Las plataformas de comercio electrónico enfrentan diferentes obligaciones que sus contrapartes físicas, como la supervisión y verificación de información, que puede presentar un mayor nivel de responsabilidad. Dependiendo de condiciones específicas del mercado y el clima empresarial local, pueden haber diferentes enfoques que se adapten a las necesidades de las empresas, el consumidor y el gobierno. En los mercados maduros con una alta concentración de negocios, es probable que se necesiten obligaciones más estrictas y que se entiendan bien. Sin embargo, obligaciones similares en mercados más pequeños y más fragmentados podrían demorar o poner en desventaja a los nuevos participantes en las plataformas listas para el comercio electrónico, como ha sido el caso en las economías en la Asociación de Naciones del Sudeste Asiático (ASEAN).

- **Resolución de disputas:** Los mecanismos de resolución de disputas son particularmente importantes, ya que las disputas entre comerciantes y clientes y las disputas B2B tienen lugar con frecuencia en las transacciones digitales. Si bien el litigio (incluso a través de tribunales de reclamos pequeños) es una posibilidad, puede no ser la mejor opción en todas las jurisdicciones. La ODR provista por agentes públicos o privados, así como la mediación y arbitraje, pueden ser enfoques más eficaces para resolver disputas de manera eficiente.

- **Derecho a revocar/período de reflexión:** Otra área de prioridad para las empresas y consumidores es el derecho a revocar/cancelar (período de reflexión), que permite a los consumidores cancelar pedidos en línea dentro de cierto período de tiempo. La duración exacta del período varía según las jurisdicciones, y la comunidad empresarial debe familiarizarse con las excepciones al derecho a revocar. La defensa se puede personalizar según las necesidades de los sectores específicos.

- **Estructuras institucionales para regular la protección del consumidor en el comercio electrónico:** En muchos países, aún se debe establecer un organismo regulatorio específico para la protección del consumidor en el comercio electrónico. Tener un organismo regulador dedicado puede ayudar a asegurar que las regulaciones reflejen las necesidades del mercado local y pueden proporcionar a las empresas un punto de enfoque para los esfuerzos de defensa. Un enfoque es la creación de unidades especiales de protección del consumidor dentro de una institución reguladora existente (agencia de protección del consumidor) encargada de enfrentar los desafíos en línea.

Lista de verificación para analizar las leyes y regulaciones existentes de protección del consumidor

¿Quién regula la protección del consumidor en línea en su jurisdicción (ministerio, organismo regulador, etc.)? ¿Hay un organismo o unidad reguladora dedicada para la protección del consumidor en línea?

¿La protección del consumidor en línea ha sido incorporada en leyes de protección del consumidor existentes, o existe una ley específica de protección del consumidor en línea?

Si la respuesta es no, ¿hay nuevos proyectos de ley, regulaciones o políticas que abordan las cuestiones de protección del consumidor en línea?

¿Quién es responsable de la aplicación de la leyes y regulaciones de protección del consumidor dentro de su jurisdicción?

Cuando las disputas surgen, ¿el mecanismo de aplicación en su jurisdicción puede resolver estas cuestiones de manera justa y oportuna?

¿Su país ha adoptado o promovido un marco de resolución de disputas en línea (ODR)? ¿Los mecanismos de ODR se utilizan comúnmente dentro de la comunidad empresarial local?

¿Las empresas se autorregulan para garantizar la protección del consumidor?

¿Existen vías existentes para el diálogo público y privado sobre la protección del consumidor en línea? ¿Existen actualmente oportunidades para que el sector privado trabaje junto con organismos reguladores y responsables de formular políticas para crear y defender las leyes de protección del consumidor?

¿Se notifica a las empresas cuando se está desarrollando un proyecto de ley y existe un proceso establecido para proporcionar comentarios?

¿Se ha involucrado con marcos que regulan la protección del consumidor en el nivel regional o internacional?

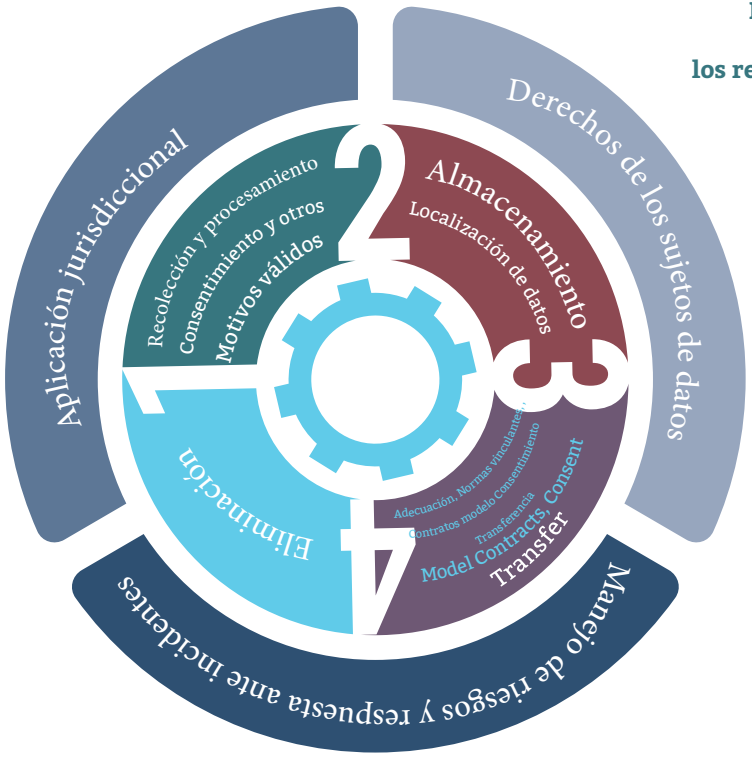
Entender el problema – Protección de datos

La economía digital ha ayudado a impulsar la creación y circulación internacional de una cantidad de datos sin precedentes. Las regulaciones de protección de datos se relacionan con las personas que compran bienes y servicio electrónicamente y las compañías que compran, vender o brindan servicios en línea protegiendo los datos que se envían a través de estas transacciones. La protección de datos tiene múltiples propósitos como privacidad y seguridad y tradicionalmente ha sido un enfoque de regulaciones nacionales, en parte, debido a fuertes preocupaciones de los gobiernos sobre la seguridad nacional.

Considerados como el aceite de la economía digital, los datos se han convertido en un producto global clave y se utilizan, procesan, intercambian y analizan cada vez más en cantidades masivas para potenciar el contenido, los bienes y los servicios digitalizados. Por lo tanto, la protección de datos se ha convertido en un punto focal para la comunidad empresarial, los organismos reguladores y los consumidores por igual. Todos los datos siguen un ciclo de vida – recopilación y procesamiento de datos, almacenamiento, transferencia y eliminación – que sustentan la mayoría de los enfoques regulatorios en todo el mundo (consulte el **Diagrama 2**). La regulación tiende a seguir estos pasos en el ciclo de vida de los datos, y las empresas pueden tener diferentes obligaciones dependiendo de su modelo comercial específico. Las regulaciones también con frecuencia incluyen obligaciones transversales, como respuestas a una violación de datos.

Los países en todo el mundo reconocen cada vez más la importancia esencial de los datos y promulgan leyes de protección de datos en respuesta. Para los gobiernos, regular los datos requiere un equilibrio delicado entre muchos factores: seguridad nacional, vigilancia,

Diagrama 2. Elementos regulatorios de los regímenes de protección de datos



Fuente: New Markets Lab (2018)

política sobre competencia, innovación, la integridad del proceso electoral y la protección del consumidor. A las personas también les preocupa cómo se recopilarán y utilizarán sus datos personales, particularmente en áreas sensibles como los datos biométricos. Por ejemplo, algunas personas pueden preocuparse por las publicidades para razones comerciales o políticas que se dirigen a estas personas sobre la base de los datos personales. Muchos también se preocupan por la vigilancia del gobierno.

Hasta julio de 2018, 107 países habían promulgado leyes de protección de datos. Otros países con grandes mercados o mercados en crecimiento de bienes y servicios digitales (como Kenia, Brasil, Nigeria y Egipto) actualmente están elaborando proyectos para proteger los datos. La participación y los comentarios a lo largo del proceso de elaboración es una manera importante para que la comunidad empresarial se exprese (consulte el estudio de caso en la página 23). Como con la protección del consumidor, no hay un estándar reconocido a nivel internacional para guiar el desarrollo de regulaciones nacionales sobre la protección de datos. Esto no solo afecta a la comunidad empresarial, que a veces debe diseñar procedimientos separados de protección de datos para cumplir con las regulaciones en diferentes jurisdicciones, sino también tiene un impacto significativo sobre la habilidad de la autoridad reguladora de aplicar las leyes de protección de datos. La falta de armonización presenta una oportunidad oportuna y un tema de controversia común para la participación pública-privada. Para participar más eficazmente en este diálogo, el sector privado podría familiarizarse con los regímenes legales de otros países que pueden servir como modelos para la legislación nacional o alentar a las responsables de formular políticas y asociaciones empresariales a enfocarse en iniciativas de políticas internacionales.

Para las empresas, los requisitos específicos para la protección de datos serán fundamentales. Por ejemplo, las regulaciones sobre el registro y tarifas no deben ser demasiado onerosas, y los requisitos de brindar controles internos como oficiales de protección de datos pueden afectar desproporcionalmente a las empresas más pequeñas. Además, el problema de la localización de datos (requisitos que las compañías deben desarrollar centros de datos locales para almacenar los datos o, en algunos casos, guardar una copia de los datos localmente) se ha abordado con criticismo por parte del sector privado.

Las compañías de todos los tamaños quieren aprovechar la cantidad masiva de datos disponibles para brindar bienes y servicios innovadores y, como se señaló en una publicación reciente de CIPE, pueden usar sistemas sólidos de protección de datos para impulsar la reputación de la marca y desarrollar confianza entre consumidores y usuarios[9]. A nivel mundial, están surgiendo puntos en común sobre cómo proteger los intereses de las pequeñas empresas y los consumidores, y a la vez promover la innovación y el crecimiento. Los grupos de defensa que trabajan con PyMEs y empresas más grandes pueden usar estos enfoques para desarrollar una agenda diversa.

Las diferencias en el grado en que los países regulan la protección de datos también afecta los flujos de datos transfronterizos, que tienden a reflejar uno de los dos enfoques principales, cada uno con diferentes implicancias para el sector privado: 1) **un enfoque centrado en la adecuación de las regulaciones en el país que exporta los datos**, que hace hincapié en la solidez del régimen legal del país y pone la carga en el sector público, o 2) **un enfoque de normas corporativas vinculantes**, que evalúa el grado en el que una compañía cuenta con un mecanismo de revisión independiente eficaz para proteger los datos y coloca una carga en el sector privado. Si bien lo último puede parecer menos atractivo, no es necesariamente una mala opción.

9. *CIPE, Why Companies in Emerging Markets Should Prioritize Data Privacy. Web. 6 de abril de 2018 017.*

Estudio de caso:
Comentarios sobre las leyes de protección de datos de Panamá

Las asociaciones empresariales puede participar activamente en el proceso de legislación para las leyes de protección de datos. Si bien el proceso en sí mismo varía considerablemente en las jurisdicciones, los procesos administrativos a veces permiten la participación y comentarios de la sociedad civil y los agentes privados. Un ejemplo es el desarrollo de una legislación de protección de datos en Panamá.

A mediados de 2016, el Congreso de Panamá presentó un proyecto para regular la protección de datos en el país. Celebró una audiencia pública de tres meses para recibir comentarios de agentes de la sociedad civil, ciudadanos privados y empresas. La audiencia pública fue realizada por la Autoridad Nacional para la Innovación Gubernamental y la Autoridad Nacional de Transparencia y Acceso a la Información, y tuvo la participación especial de la Organización de los Estados Americanos y el Tribunal Interamericano de Derechos Humanos, lo que significa que se consideraron marcos regionales e internacionales. Los participantes brindaron comentarios, que se incluyeron en el proyecto final presentado al Congreso de Panamá en febrero de 2017. Para promover el debate público sobre el tema, diferentes organizaciones realizaron conferencias con un representante grande del sector privado (como Google) y la Cámara de Comercio de Panamá.

Hasta 2018, el proyecto no ha sido adoptado como ley debido a limitaciones de presupuesto. Sin embargo, el proceso de elaboración de normas en Panamá destaca una buena práctica por la cual las asociaciones empresariales interesadas pueden participar activamente en el proceso de elaboración de normas y expresar sus inquietudes, y se involucraron instituciones y compañías regionales e internacionales para contribuir con opiniones adicionales y apoyar el diálogo. De manera similar, en India y Kenia, los proyectos de protección de datos se encuentran actualmente abiertos para comentarios públicos.

Fuentes: IPANDETEC, Cronología de un Proyecto de Ley de Protección de Datos en Panamá, 29 de enero de 2018. Web; AIG, Consulta pública sobre Proyecto de Ley de Protección de Datos de Carácter Personal" refuerza el marco legal para la Economía y el Gobierno Digital, 11 de julio de 2016, Web. Violeta Villar, Panamá necesita aprobar Ley de Protección de Datos, El Capital, 14 de febrero de 2018. Web; Gobierno de Panamá, Avalan proyecto que establece la protección de datos de carácter personal, Consejo de Gabinete, 18 de enero de 2017, Web.

Guía para empresas y recomendaciones

Como primer paso, las comunidades empresariales locales deben entender el rango de leyes, regulaciones y otras medidas que son aplicables con respecto a la protección de datos; esto dependerá de dónde residen los sujetos de los datos involucrados y las etapas relevantes en el ciclo de vida de los datos (recopilación, procesamiento, almacenamiento o transferencia). Debido a la falta de armonización internacional, las empresas locales pueden estar sujetas a leyes y regulaciones en múltiples jurisdicciones. Las compañías pueden necesitar diseñar sistemas de protección de datos separados, como términos de servicio, para acomodar los diferentes requisitos nacionales de regulación. Si bien este puede no ser un problema para empresas más grandes, pone un peso pesado en las PyMEs. Trabajar en colaboración mediante asociaciones empresariales o cámaras de comercio puede ser una manera eficaz para que las PyMEs aseguren que se consideren sus necesidades particulares.

Los defensores de la comunidad empresariales también deben unirse con un enfoque común con respecto a la transferencia de datos transfronterizos. Hay varias consideraciones notables, con implicancias para aquellos en la comunidad empresarial que buscan expandirse en mercados extranjeros. En primer lugar, si las leyes de protección de datos aplican únicamente a nivel nacional o si también alcanza a las empresas extranjeras cuando recopilan o procesan datos de residentes nacionales (el sistema de Japón es un ejemplo de lo último). Una segunda consideración es el grado en que la comunidad empresarial local o los responsables de formular políticas nacionales participan en discusiones más amplias a nivel internacional. Los defensores pueden presionar para una mayor armonización internacional o un enfoque sostenible en que los marcos e instituciones nacionales incorporen mejor las necesidades de las PyMEs, por ejemplo. Con respecto a la armonización regulatoria, existen algunos buenos modelos – por ejemplo, esfuerzos para simplificar las certificaciones entre la Unión Europea (UE) y APEC – pero aún no están muy difundidos.

A medida que la comunidad empresarial local explora el panorama legal y regulatorio para la protección de datos, seis consideraciones regulatorias principales podrían ayudar a estructurar los modelos empresariales e informar los esfuerzos de defensa. Son 1) **el alcance del régimen regulatorio**, 2) **el grado en que las leyes de protección de datos se enfocan en el consumidor**, 3) **los niveles de protección de datos que varían según el tamaño de la compañía**, 4) **las estructuras institucionales para regular la protección de datos**, 5) **los enfoques para las transferencias transfronterizas**

- **Alcance del régimen regulatorio:** Los regímenes regulatorios para la protección de datos varían y se pueden personalizar según la naturaleza del mercado local. Por ejemplo, mientras que algunos países han adoptado regulaciones generales más completas sobre la protección de datos (como la UE, Japón y Ghana), otros regulan de acuerdo con las necesidades de protección de datos de los diferentes sectores o funciones. Corea del Sur es un ejemplo de lo último, con diferentes leyes que aplican a la tecnología de la información (IT), transacciones financieras y la divulgación de información personal de crédito[10]. Mientras que Brasil actualmente tiene un enfoque similar, hay dos proyectos de leyes bajo consideración que llevarían al país hacia un marco general de protección de datos[11]. A medida que más jurisdicciones comienzan a cambiar o actualizar sus marcos legales, la participación del sector privado en el proceso de elaboración de normas será cada vez más importante.

- **Enfoque en el consumidor:** Algunos marcos legales influyentes, como la Regulación de Protección de Datos Generales (GDPR, por sus siglas en inglés) de la UE[12], adoptan un enfoque centrado en el consumidor con respecto a la protección de datos que requiere que las empresas brinden más control y un rango de derechos a los consumidores. Por ejemplo, en la UE y Rusia, requisitos más estrictos aplican a los datos sensibles. Ciertas categorías de consumidores, como los niños, también pueden tener niveles más altos de protección (por ejemplo, la Ley de Derechos de los Niños N.º 26 de 20013 en Nigeria protege la privacidad de los niños menores de 18 años). La comunidad empresarial puede aprender de estos ejemplos e incorporar información clave como apropiada dentro de su jurisdicción.

- **Niveles de cumplimiento que difieren según el tamaño de la compañía:** La capacidad y el impacto de los datos de la comunidad empresarial también es una consideración común; algunas jurisdicciones han creado leyes y regulaciones con diferentes niveles de cumplimiento para acomodar la capacidad de empresas de diferentes tamaños. Por ejemplo, en Australia, las empresas con una facturación anual de $3 millones de dólares australianos o menos (con ciertas excepciones) no están sujetas a la Ley de Privacidad. Esta es una consideración especialmente relevante para las PyMEs y las nuevas empresas.

10. *DLA Piper, Data Protection Laws of the World: South Korea. Web. 16 de enero de 2017*
11. *Bruno Bioni and Renator Leite Monteiro. Brazilian General Bill on the Protection of Personal Data. IAPP. Web. 31 de enero de 2018; Bill 5276/2016 Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Web.*
12. *Regulation (EU) 2016/679 of The European Parliament and Of The Council Of 27 April 2016 on The Protection of Natural Persons with Regard to The Processing Of Personal Data And on The Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).*

- **Estructuras institucionales para regular la protección de datos:** El establecimiento de una clara institución reguladora responsable de la protección de datos puede brindar un punto de contacto para la comunidad empresarial y el público, racionalizar las normas y evitar desafíos y costos debido a regulaciones que se superponen. En algunas jurisdicciones, se han fundado nuevas entidades reguladoras o unidades especiales dentro de las instituciones reguladoras existentes para abordar los desafíos específicos relacionados con la protección de datos. Estas unidades pueden estar limitadas con respecto a la duración y alcance, y apoyar los esfuerzos de avanzar hacia un sistema más general de regular la protección de datos.

- **Enfoques sobre las transferencias transfronterizas de datos:** El mejor enfoque para las transferencias transfronterizas de datos puede depender en última instancia en la fuerza de las leyes nacionales de protección de datos. En jurisdicciones con leyes de protección de datos débiles, la comunidad empresarial local puede, en realidad, preferir el enfoque de normas corporativas vinculantes, que confían en que las compañías implementen mecanismos internos y puede dar lugar a una aplicación más estricta[13]. Por el otro lado, si una empresa está ubicada en una jurisdicción con normas fuertes de protección de datos, puede solicitar que su gobierno busque el "estado de adecuación" de otra jurisdicción, lo que racionalizaría la transferencia de datos en general.

- **Excepciones a los regímenes de protección de datos:** En las jurisdicciones donde los requisitos de protección de datos pueden poner una carga de cumplimiento en las empresas, particularmente las PyMEs, la comunidad empresarial podría recomendar excepciones a ciertas normas y trabajar con los gobiernos para modificar estos requisitos. Otras excepciones para considerar incluyen nombramiento de un oficial interno de protección de datos (basado en el tamaño de la compañía), reducción de costos de registro excesivos, o eliminación de requisitos de localización de datos.

13. *El enfoque de contratos modelo, que considera la redacción en los contratos específicos y determinar si protege lo suficiente la transferencia de datos, también sería una opción, pero se utiliza con menos frecuencia (hasta la fecha, solo se usa en la UE y depende de la completa implementación de contratos modelo). Consulte United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development. 13. Web. 2016.*

Lista de verificación para analizar las leyes y regulaciones existentes de protección de datos

¿Quién regula la protección de datos en línea en su jurisdicción (ministerio, organismo regulador, etc.)?

¿Su país o territorio tienen leyes o regulaciones de protección de datos? ¿Proyectos de leyes o regulaciones?

Si su jurisdicción tiene una ley o leyes de protección de datos, ¿el ministerio/organismos reguladores tienen un enfoque más general con respecto a la protección de datos, o los diferentes sectores se regulan de manera diferente?

¿Quién es responsable de la aplicación de la leyes y regulaciones de protección de datos dentro de su jurisdicción?

¿Su sector o industria se preocupa más por un aspecto particular del ciclo de vida de la protección de datos?

¿Su sector o industria se preocupa más por un sector demográfico particular del usuario?

¿Las empresas se autorregulan para garantizar la protección de datos? ¿Existe un mecanismo para rectificar las violaciones de datos públicamente?

¿Existen vías existentes para el diálogo público y privado sobre la protección de datos en línea? ¿Existen actualmente oportunidades para que el sector privado trabaje junto con organismos reguladores y responsables de formular políticas para crear y defender las leyes de protección de datos?

¿Se ha involucrado con marcos que regulan la protección de datos en el nivel regional o internacional?

¿Ha tenido problemas con respecto a la protección de datos transfronterizos? Si la respuesta es sí, ¿sabe cómo se han abordado?

Entender el problema – Ciberseguridad

La regulación de ciberseguridad, que protege la tecnología de la información y los sistemas informáticos contra ataques, es una preocupación global importante para todos los miembros de la comunidad empresarial y todos los que se involucran en actividades en línea. En años recientes, los ataques en computadoras y redes informáticas, tanto públicas como privadas, han crecido en escala y gravedad, perjudicando a gobiernos, la industria y a los consumidores. La ciberseguridad incluye los activos de los agentes públicos y privados y cubre "dispositivos de computación conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida o almacenada"[14]. Si bien la economía digital y el comercio electrónico en particular han logrado un crecimiento inclusivo, las tecnologías que se encuentran en constante evolución pueden resultar en vulnerabilidades en internet que requieren sistemas de ciberseguridad sólidos y resistentes.

El marco regulatorio para la ciberseguridad ha evolucionado en tres etapas: (1) **legislación sobre delitos informáticos en el nivel nacional**, (2) **estándares y pautas iniciadas por el sector privado**, y (3) **el cambio reciente para una legislación más amplia que regule por completo la ciberseguridad** (Consulte el Diagrama 3 abajo). La comunidad empresarial debe conocer el marco de ciberseguridad dentro de su jurisdicción local y determinar dónde puede haber brechas. Los agentes públicos y privados deben trabajar en coordinación para determinar los enfoques regulatorios apropiados y la secuencia de las reformas, tomando en cuenta la carga de cumplimiento para las empresas (particularmente las PyMEs y nuevas empresas) y las necesidades de los consumidores.

Diagrama 3. Evolución de las regulaciones de ciberseguridad

Legislación sobre delitos informáticos

Primer tipo de regulación de ciberseguridad adoptada en la mayoría a través de un enfoque descendiente. Los delitos informáticos más comunes incluyen:

- Suplantación de correo electrónico
- Fraude electrónico
- Correo no solicitado
- Difamación cibernética
- Acoso cibernético
- Robo de identidad
- Piratería de software
- Acceso no autorizado
- Negación de servicio
- Deformación de web
- Ransomware (cibersecuestro de datos)
- Ataque Salami
- Bomba lógica
- Estafa de datos

Aplicación de múltiples partes interesadas dirigidas por el sector privado

El desarrollo privado de un programa, procedimientos y estándares de ciberseguridad se institucionaliza a través de un marco de múltiples partes interesadas

Regulación integral de ciberseguridad

Las regulaciones generales recientemente promulgadas abordan:

- Cobertura (general o específica del sector)
- El aspecto preventivo (mecanismos estratégicos, organizacionales y de monitoreo), y
- El aspecto reactivo (definición de incidente cibernético o ataque cibernético y las obligaciones legales impulsadas por el incidente cibernético o el ataque cibernético)

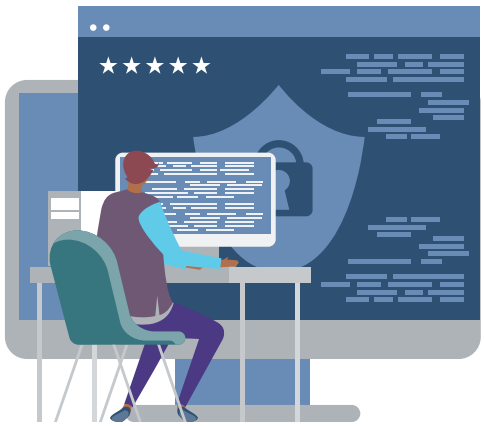
Fuente: New Markets Lab (2018)

14. *International Telecommunications Union, Definition of Cybersecurity. Web.*

La legislación sobre el delito informático, que penaliza un rango de delitos digitales como hackeo y robo de identidad, es el enfoque más común y puede ser el más efectivo cuando está acompañada por sanciones apropiadas y una aplicación estricta. La comunidad empresarial local puede ayudar a enfocar y priorizar intervenciones alineando las buenas prácticas de la industria con el régimen legal y a través de iniciativas públicas-privadas. La comunidad empresarial debe considerar el propósito de la política detrás del movimiento reciente para la promulgación de regulaciones integrales de ciberseguridad, así como las potenciales cargas. Los organismos reguladores probablemente continúen implementando normas y estándares más estrictos y detallados, que fortalecerán la ciberseguridad y también crearán obligaciones de cumplimiento adicionales. Será importante para la comunidad empresarial local presionar a los organismos reguladores para que encuentren el equilibrio correcto.

La legislación sobre ciberseguridad que sea integral pero que no tenga un alcance excesivo podría incluir los siguientes componentes: designación de entidades que son esenciales para la seguridad nacional con requisitos equilibrados para esas entidades y sus sistemas de información; enfoques basados en la gestión de riesgos para compañías en línea con las buenas prácticas globales que toman en cuenta la estructura y los activos; y medidas para reducir la frecuencia y magnitud de los ataques cibernéticos en los sistemas clave para el crecimiento económico. Las disposiciones externas para tener en cuenta en la legislación sobre ciberseguridad incluyen una obligación de monitorear la expresión en línea, auditorías previas al lanzamiento de hardware o software, largas sentencias penales por incumplimiento y requisitos de localización de datos. Además, establecer Equipos de Respuesta para Emergencias Informáticas (CERT, por sus siglas en inglés), común en todo el continente americano, puede facilitar los esfuerzos de recuperación e informe de incidentes para la comunidad empresarial y para la infraestructura crítica y las agencias gubernamentales[15].

Los enfoques excesivamente prescriptivos pueden presentar desafíos para la comunidad empresarial, que serían mejor atendidos por un sistema que permita flexibilidad para adoptar estándares relevantes. Tanto la comunidad empresarial como los organismos reguladores podrían beneficiarse de la creación de incentivos para que las empresas adopten buenas prácticas. Este enfoque ascendente pondría una carga menor de cumplimiento en los organismos reguladores, y a la vez permiten que las PyMEs desarrollen capacidad para mejorar la confianza del consumidor. Reconocer la equivalencia de los estándares existentes comparables también aliviaría la carga regulatoria en la comunidad empresarial local. Fundamentalmente, la comunidad empresarial debería participar en la toma de decisiones y el proceso de armonización para garantizar que se aborden las necesidades (consulte el caso de estudio a continuación). La comunidad empresarial también podría buscar marcos internacionales y regionales para guiar la aplicación de las buenas prácticas y ayudar a definir su enfoque de defensa.



15. *https://www.sites.oas.org/cyber/EN/Pages/Directory/Default.aspx*

Estudio de caso:

Ciberseguridad de coordinación pública-privada en Túnez

En Túnez, se creó la Agencia Nacional de Seguridad Informática (NACS, por sus siglas en inglés) en 2003 bajo el Ministerio de Tecnologías de la Comunicación. La NACS tiene la responsabilidad de ejecutar la estrategia nacional en seguridad de ICT (Tecnología de Información y Comunicación), llevar a cabo evaluaciones de riesgo periódicas y establecer el Centro de Coordinación de Túnez Cert (Cert-TCC, por sus siglas en inglés) que brinda asistencia con la seguridad de la información. Cert-TCC tiene múltiples misiones, incluso informar al público sobre incidentes y amenazas cibernéticas, promover el desarrollo de capacidad y asistir a las comunidades nacionales, regionales e internacionales para identificar vulnerabilidades de productos y sistemas.

Más prometedor para la comunidad empresarial, el Cert-TCC también tiene la responsabilidad de facilitar la comunicación entre los agentes del sector público y privado, en particular expertos y profesionales en el campo de la tecnología y asociaciones empresariales enfocadas en la ciberseguridad. Cert-TCC ha ayudado a establecer foros de debate y programas de desarrollo de capacidad para conectar a estas diferentes partes interesadas. El Cert-TCC también promovió la cooperación pública-privada a través de Saher-HoneyNet, una iniciativa que usa un enfoque preventivo para mitigar las amenazas cibernéticas y también promueve la aplicación entre las agencias.

Sin embargo, queda mucho por hacer para alinear el enfoque de Túnez con los estándares internacionales de ciberseguridad. La comunidad empresarial en Túnez puede alentar a su gobierno que realice más esfuerzos de desarrollo de capacidad para fortalecer el cumplimiento con los estándares internacionales.

Fuentes: Tunisian National Agency for Computer Security. History of The Creation of The Agency Web; Jidaw, Tunisia Information Security strategy – National Agency for Computer Security. Web.

Guía para empresas y recomendaciones

Un sistema de ciberseguridad sólido y resistente es esencial para abordar las vulnerabilidades en internet. Las regulaciones en este cambio han evolucionado a través de tres etapas, como se mencionó arriba, y los agentes públicos y privados deben trabajar en colaboración para determinar, adoptar e implementar el equilibrio apropiado de regulaciones y flexibilidad. Este proceso debe tomar en consideración la carga de cumplimiento para la comunidad empresarial local (particularmente las PyMEs y nuevas empresas), objetivos de política y las necesidades de los consumidores y ciudadanos.

A medida que la comunidad empresarial local explora el panorama legal y regulatorio para la ciberseguridad, cinco consideraciones regulatorias principales podrían ayudar a estructurar los modelos empresariales e informar los esfuerzos de defensa. Son 1) **el alcance del régimen regulatorio de ciberseguridad**; 2) **incentivos para adoptar buenas prácticas de la industria**; 3) **estructuras institucionales para regular la ciberseguridad**; 4) **mejor aplicación de los marcos de ciberseguridad**; y 5) participación en los marcos internacionales y regionales.

- **Alcance del régimen regulatorio de ciberseguridad:** Los regímenes regulatorios para la ciberseguridad varían en las tres fases principales que se trataron arriba (ley de delitos informáticos, aplicación de múltiples partes interesadas dirigidas por el sector privado y leyes integrales de ciberseguridad). Por ejemplo, muchos países tienen leyes sobre el delito informático, pero aún están desarrollando leyes generales de ciberseguridad. A medida que más jurisdicciones comienzan a cambiar o actualizar sus marcos legales para la ciberseguridad, la participación del sector privado en el proceso de elaboración de normas será cada vez más importante. Los diálogos públicos-privados podrían beneficiar un rango más amplio de partes interesadas, incluso defensores de internet abierta e instituciones financieras, y la comunidad empresarial local debería determinar si existen canales apropiados para estos diálogos en el nivel nacional.

- **Incentivos para adoptar buenas prácticas de la industria:** A medida que los sistemas legales formales cambian a un enfoque integral en la ciberseguridad, los esfuerzos liderados por la industria basados en buenas prácticas pueden ser una manera importante para abordar las inquietudes sobre la ciberseguridad e impulsar la confianza del consumidor. Las buenas prácticas pueden intercambiarse a través de enfoques como iniciativas de múltiples partes interesadas, pautas claras de implementación y la adopción personalizada de leyes y regulaciones modelo. Estas iniciativas podrían ayudar a las empresas a obtener más información sobre los estándares y priorizar los pasos para adoptar buenas prácticas, que serían particularmente útil para las PyMEs con capacidad limitada y falta de inversión en ciberseguridad. Los organismos reguladores también podrían crear incentivos para que las empresas adopten buenas prácticas (por ejemplo, pautas voluntarias y programas de certificación).

- **Estructuras institucionales para regular la ciberseguridad:** El establecimiento de un único organismo regulador para administrar todas las funciones institucionales relacionadas con la ciberseguridad podría facilitar el cumplimiento, simplificar la regulación, desarrollar capacidad (tanto en el sector público como en el privado) y evitar desafíos y costos debido a regulaciones que se superponen. Los ejemplos de algunas jurisdicciones, como Túnez, que ha creado un organismo regulador central, y Sri Lanka, donde se han fundado unidades específicas del sector para superar desafíos específicos, podrían proporcionar puntos de debate útiles para la participación pública-privada.

- **Mejor aplicación de los marcos de ciberseguridad:** También es un punto clave la aplicación adecuada de los marcos existentes de ciberseguridad en todos los niveles (nacional, regional e internacional). Esto debe incluir defensa de colaboración y armonización entre las diferentes agencias de aplicación responsables de diferentes aspectos de ciberseguridad y mayor cooperación internacional.

- **Mejores marcos internacionales y regionales:** La comunidad empresarial podría promover el fortalecimiento de marcos internacionales y regionales, que tienden a ser generales y centrarse en torno al desarrollo de capacidad e intercambio de información. Si bien es importante, estos son solo los primeros pasos y no es suficiente para abordar las preocupaciones globales con respecto a la ciberseguridad. Un mayor enfoque internacional también podría facilitar la elaboración de normas nacionales y vincular las tres etapas de la regulación de la ciberseguridad (leyes sobre el delito informático, iniciativas lideradas por el sector privado y legislación integral de ciberseguridad) para guiar a los países que se encuentran en las diferentes etapas de desarrollo.

Lista de verificación para analizar las leyes y regulaciones existentes de ciberseguridad

¿Quién regula la ciberseguridad en su jurisdicción (ministerio, organismo regulador, etc.)? ¿Hay un solo organismo regulador que maneja todas las cuestiones relacionadas con la ciberseguridad o las funciones se dividen entre instituciones?

¿Su jurisdicción tiene leyes sobre (1) delito informático o (2) la ciberseguridad más en general? ¿Existe una ley de seguridad nacional que aborde los aspectos de la ciberseguridad?

Si la respuesta es no, ¿hay proyectos de ley en consideración para abordar los aspectos de la ciberseguridad?

¿Quién es responsable de la aplicación de las leyes y regulaciones relacionadas con la ciberseguridad en su jurisdicción? ¿Existen sanciones apropiadas para disuadir el incumplimiento pero que no sean excesivas como para disuadir el informe?

¿Existen pautas voluntarias y programas de certificación que guian la autorregulación de la industria?

¿Qué requisitos de hardware, software y organizacionales para abordar la ciberseguridad se aplican a la comunidad empresarial local?

¿Existen vías existentes para el diálogo público-privado sobre los enfoques rentables de la ciberseguridad? ¿Existen actualmente oportunidades para que el sector privado trabaje junto con organismos reguladores y responsables de formular políticas para crear y defender las leyes de ciberseguridad?

¿Se notifica a las empresas cuando se está desarrollando un proyecto de ley y existe un proceso establecido para proporcionar comentarios?

¿Se ha involucrado con marcos que regulan la ciberseguridad en el nivel regional o internacional?

Entender el problema – Transacciones electrónicas (pagos electrónicos y firmas electrónicas)

El comercio electrónico sustenta una gran parte de la economía digital. El comercio electrónico es similar al intercambio tradicional de bienes y servicio e incluye transacciones digitales y acuerdos entre agentes en la cadena de suministro. Dentro de las transacciones electrónicas, surgen distintas cuestiones, por ejemplo, cómo celebrar un contrato justo o recibir pago sin la interacción cara a cara o cómo resolver disputas entre partes. Esta sección de la Guía cubre dos áreas de particular importancia para las transacciones electrónicas: los pagos electrónicos (e-payments) y las firmas electrónicas (e-signatures).

Los pagos electrónicos son una parte esencial de la realización de negocios para toda compañía y el consumidor que participan en transacciones en línea, y las firmas electrónicas son el elemento fundamental del contrato electrónico, que ahora está surgiendo como sustituto de los contratos manuales. Tanto los pagos electrónicos como las firmas electrónicas implican diferentes desafíos y dificultades, y la comunidad empresarial debe mantenerse involucrada en el proceso de elaboración de normas y comunicarse abiertamente con el gobierno para garantizar que se aborden sus necesidades.

Pagos electrónicos

Los pagos electrónicos son una parte integral de la economía digital y han sido ampliamente adoptados en años recientes gracias a la innovación de la tecnología y la penetración masiva de teléfonos móviles y teléfonos inteligentes en todo el mundo. Hay muchos tipos de sistemas de pago electrónico, pero se pueden clasificar ampliamente en uno de dos grupos: pagos electrónicos relacionados bancario y pagos electrónicos no bancarios. Los pagos electrónicos bancarios incluyen los pagos electrónicos más tradicionales como la Cámara de Compensación Automatizada (ACH, por sus siglas en inglés) y tarjetas de crédito y débito y se conectan a sistemas bancarios a través de diferentes tipos de cuentas bancarias. Los pagos electrónicos no bancarios se brindan a través de intermediarios no bancarios que incluyen métodos más nuevo y más innovadores como PayPal, Alipay y Google Wallet.

Los pagos electrónicos no están exentos de desafíos, especialmente cuando se opera a través de fronteras y sistemas financieros. Ambas partes de una transacción quieren asegurarse de que los pagos se realizarán sin demora, y los gobiernos deben garantizar que las transacciones protejan a aquellos con menos poder en el mercado. Las prioridades comunes para el sector público y privado incluyen prevención de fraude, y cuestiones de seguridad en el nivel de la transacción. Como resultado de las diferentes partes interesadas y consideraciones involucradas, los organismos reguladores tienden a enfocarse en regulaciones para los pagos electrónicos. Dar prioridad al desarrollo de la infraestructura institucional que pueda investigar problemas a medida que surgen y hacer cumplir las normas en caso de una violación es también una consideración clave para los gobiernos.

Dependiendo del tipo de sistema de pago electrónico que se utilizan, hay varios enfoques para las regulaciones (consulte el **Diagrama 4** de arriba). En general, los pagos electrónicos bancarios están regulados estrictamente en todo el mundo, y los responsables de formular políticas tienden a usar elementos similares (prevención y cumplimiento, autenticación de las transacciones, investigación y aplicación). En contraste, los sistemas regulatorios para los pagos electrónicos no bancarios a menudo siguen uno de dos enfoques: 1) un **enfoque ex ante** que contiene requisitos para ingresar y operar en el mercado a través de una aprobación regulatoria según el caso o medidas más amplias, y 2) un **enfoque ex post** que utiliza condiciones menos restrictivas para ingresar al mercado, y se centra más en la aplicación una vez que las empresas están operando en el mercado.

Diagrama 4. Enfoques regulatorios sobre el pago electrónico

Fuente: New Markets Lab (2018)

Firmas electrónicas

Las normas claras con respecto a las firmas electrónicas – que, como las firmas manuales, indican que las partes celebran un contrato aplicable – son cada vez más importantes en la economía digital. Los sistemas regulatorios con respecto a las firmas electrónicas brindan la seguridad de que las obligaciones del comprador y del vendedor son válidas, legales y aplicables. No obstante, la comunidad empresarial local no solo debe considerar el marco legal en sí mismo, sino también centrarse en su implementación, ya que las firmas electrónicas, a veces, siguen siendo consideradas de manera diferente a pesar de los marcos legales que las reconocen.

En general, las firmas electrónicas están reguladas de tres maneras diferentes: 1) las **regulaciones tecnológicamente neutrales** consideran que todos los tipos de firmas electrónicas y firmas manuales son iguales; 2) las **regulaciones de dos niveles** reconocen la legalidad y validez de múltiples tipos de firmas electrónicas, pero consideran que las firmas digitales autenticadas por ciertas tecnologías son legalmente más significativas; y las 3) **regulaciones de tecnología específica** reconocen solo ciertos tipos limitados de firmas electrónicas (estas son regulaciones prescriptivas). Este marco institucional para hacer cumplir las firmas electrónicas varía dependiendo de qué enfoque regulatorio sigue la jurisdicción y puede incluir organismos de certificación.

Si bien las firmas electrónicas son cada vez más reconocidas, algunos organismos reguladores (por ejemplo, Sri Lanka) y tribunales en diferentes jurisdicciones (por ejemplo, Ghana) han demostrado resistencia con respecto a aceptar las firmas electrónicas, haciendo hincapié en la necesidad de una mayor participación de múltiples partes interesadas (consulte el estudio de caso en la página 37). A nivel internacional, la mayoría de los instrumentos que regulan los contratos electrónicos y las firmas electrónicas reconocen la equivalencia funcional entre las firmas manuales y las firmas electrónicas y apuntan a armonizar leyes nacionales. La Comisión de las Naciones Unidas sobre la Ley de Comercio Internacional (UNCITRAL, por sus siglas en inglés) ha desarrollado una ley modelo que proporciona orientación sobre la armonización de las normas bajo un enfoque neutral desde el punto de vista tecnológico, que facilitaría el comercio digital y atendería mejor las necesidades de la comunidad empresarial en mercados emergentes y fronterizos.

Diagrama 5. Enfoques regulatorios sobre la firmas electrónica

Fuente: New Markets Lab (2018)

Estudio de caso:
Firmas electrónicas en Sri Lanka

En 2006, Sri Lanka promulgó la Ley de Transacciones Electrónicas. N.º 19 (ETA, por sus siglas en inglés), que reconoció la legalidad y validez de las firmas electrónicas; sin embargo, la "resistencia burocrática al cambio y el letargo administrativo" impidió la implementación de la Ley durante 10 años. Este es un excelente ejemplo de una cuestión calve en la reforma legal: la diferencia entre promulgar una ley y su implementación.

Verité Research, un grupo de expertos interdisciplinarios y socio de CIPE, trabajó con la Sección de Importaciones de la Cámara de Comercio de Ceylon (CCC, por sus siglas en inglés) para promover la implementación de la ETA de Sri Lanka, que autoriza el uso de firmas digitales y documentos digitales en procesos de exportación e importación. En consulta con los miembros de CCC, Verité descubrió que los exportadores de Sri Lanka continuaba enfrentando requisitos onerosos para presentar copias impresas de documentos comerciales, y pocos líderes empresariales conocían las disposiciones de la ETA. Después de muchas reuniones con partes interesadas en empresas, la legislatura y el servicio civil, Verité y CC elaboraron y distribuyeron un informe de política. El informe y las discusiones relacionadas crearon conciencia entre los exportadores y los funcionarios gubernamentales de que las disposiciones que autorizan los documentos electrónicos y las firmas electrónicas dentro de la ETA superan otras leyes que requieren firmas manuales para la autenticación.

Verité y CCC se reunieron con funcionarios del gobierno, incluso el Comité Nacional de Facilitación del Comercio para tratar los hallazgos del informe y las recomendaciones clave. Como resultado, los presupuestos de 2017 y 2018 incluyeron propuestas para digitalizar los sistemas gubernamentales y el gobierno reformó una ordenanza de aduanas de 148 años allanando el camino para plataformas de procesamiento de documentos electrónicos (e-document) y procedimientos aduaneros más cortos. Estas mejoras podrían, en última instancia, conducir a un aumento de la competitividad comercial general de Sri Lanka.

Fuente: Financial Times, Accepting E-Documents with E-Signatures: A Small Step for the Govt, A Giant Leap for The Country. Web. 2017; Lanka Business Online, Verité Wants Govt to Issue Guidelines on E-Signature. Web. 2017.

Guía para empresas y recomendaciones

Pagos electrónicos

Los enfoques existentes con respecto a los pagos electrónicos deben equilibrar diferentes consideraciones de política y partes interesadas. Las opciones de pago electrónico pueden involucrar altos costos de cumplimiento con implicaciones negativas para la viabilidad de las empresas, particularmente cuando las empresas más pequeñas dependen de servicios de terceros. Si bien algunos aspectos de la regulación de pagos electrónicos afectan fuertemente las empresas que brindan servicios de pagos electrónicos, la información que se incluye en esta Guía aplica a la comunidad empresarial en general. Las normas relacionadas con los tipos de servicios de pago electrónico disponibles en el mercado y el grado en que se ajustan a las necesidades comerciales afectarán directamente a todas las empresas que participan en el comercio electrónico. Asimismo, las regulaciones relevantes aplicables a las instituciones bancarias, que tienden a estar fuertemente reguladas en todo el mundo, afectarán la disponibilidad de soluciones de pago bancario.

En algunas jurisdicciones, el ingreso al mercado está fuertemente regulado (regulación ex ante), mientras que en otras, se espera que las empresas se autorregulen, con el sector público muy enfocado en la aplicación. Incluso en las jurisdicciones que siguen un enfoque ex ante, la comunidad empresarial local podría trabajar con los organismos reguladores para establecer "Entornos Regulatorios de Prueba" para probar sus productos sin incertidumbre legal. Los entornos regulatorios de prueba brindan espacios seguros para que la comunidad empresarial experimente con estructuras y productos comerciales más innovadores. También promueven servicios innovadores de menor costo y ayudan a los productores a ingresar al mercado más rápido. Muchas jurisdicciones ya utilizan este modelo, y también se podría adaptar a nuevos mercados.

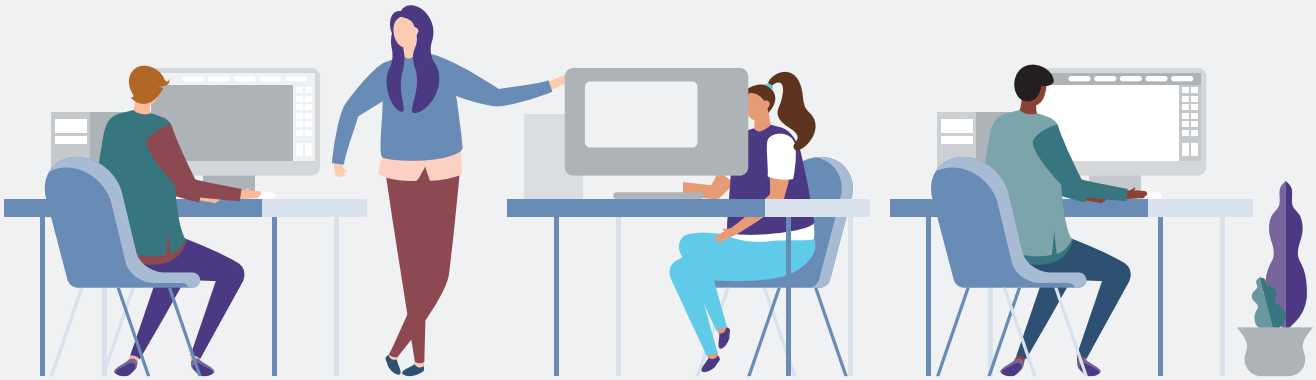
A medida que la comunidad empresarial local explora el panorama legal y regulatorio para los pagos electrónicos, cuatro consideraciones regulatorias principales podrían ayudar a estructurar los modelos empresariales e informar los esfuerzos de defensa. Son 1) **el rango de regulaciones aplicables**; 2) **estructuras institucionales para regular los pagos electrónicos**, 3) **experimentación regulatoria** (y "Entornos Regulatorios de Prueba"); y 4) **mayor participación en los marcos internacionales y regionales**.

- **Estructuras institucionales para regular los pagos electrónicos:** Si bien los pagos electrónicos tienden a estar cubiertos bajo instituciones regulatorias existentes, sería beneficioso un mayor enfoque en los desafíos particulares que surgen en un contexto de pago electrónico. Algunas jurisdicciones han creado nuevas entidades regulatorias o unidades especiales dentro de las instituciones existentes para centrarse específicamente en pagos electrónicos, y estos enfoques institucionales podrían brindar puntos de debate útiles para el diálogo público-privado.

- **Rango de regulaciones aplicables:** Los pagos electrónicos tienden a estar cubiertos bajo varios esquemas regulatorios, que abarcan tanto los pagos bancarios (que se relacionan con un rango complejo de regulaciones financieras) y pagos no bancarios. La comunidad empresarial local que utiliza (o provee) soluciones de pago bancario debe conocer el rango de regulaciones aplicables y los requisitos de cumplimiento relacionados. Si bien las opciones de financiación no bancaria tienden a estar menos reguladas, la línea entre las finanzas bancarias y no bancarias no siempre es clara. La comunidad empresarial debe trabajar con organismos reguladores para entender mejor esta división y, cuando sea relevante, alejar a los organismos reguladores de los marcos complicados, siguiendo las pautas de las jurisdicciones más flexibles.

- **Experimentación regulatoria (y "Entornos Regulatorios de Prueba"):** Los pagos electrónicos siguen evolucionando, y el alto grado de innovación en la tecnología financiera o "FinTech" exige una mayor colaboración entre el sector público y privado. Aún existe la necesidad de llevar opciones económicas al mercado para promover la inclusión financiera. Esto puede beneficiar a las PyMEs que dependen de soluciones de pago electrónico de terceros. Una innovación, si bien es inusual, ha sido establecer "Entornos Regulatorios de Prueba" para permitir que las empresas se involucren con organismos reguladores en torno a nuevos productos y servicios dentro de un espacio seguro libre de responsabilidad legal. Ya sea en el contexto del entorno regulatorio de prueba o no, el sector privado podría fomentar la adopción de una regulación ex post menos restrictiva del mercado cuando sea posible.

- **Mayor participación en marcos internacionales:** Varios marcos internacionales se relacionan con la regulación de pagos electrónicos y pueden brindar orientación a medida que los países desarrollan regulaciones más detalladas. Además, las negociaciones en curso del Comercio de Servicios de la OMC abrirían aún más el sector de servicios financieros y proporcionarían a las empresas locales en todo el mundo opciones de pago electrónico más asequibles. Las PyMEs probablemente obtendrían beneficios significativos incluso si un grupo pequeño de miembros de la OMC se comprometería a una mayor liberalización.



Firmas electrónicas

La comunidad empresarial local también debe entender las normas con respecto a los diferentes tipos de firmas electrónicas en los diferentes mercados en donde operan, incluso las excepciones que podrían aplicar. En general, la comunidad empresarial local considerará que las regulaciones tecnológicamente
neutrales son menos complicadas, pero los enfoques regulatorios deben adaptarse a una jurisdicción específica.

A medida que la comunidad empresarial local explora el panorama legal y regulatorio para las firmas electrónicas, cuatro consideraciones regulatorias principales podrían ayudar a estructurar los modelos empresariales e informar los esfuerzos de defensa. Son 1) **el alcance del régimen regulatorios**; 2) **estructuras institucionales para regular los pagos electrónicos**; 3) **mayor aplicabilidad de los marcos de pagos electrónicos**; y 4) **adopción de marcos internacionales y regionales.**

- **Alcance del régimen regulatorio:** En general, los organismos reguladores no utilizan el mismo enfoque para diferentes tipos de firmas electrónicas, y la comunidad empresarial local debe familiarizarse con las normas y excepciones específicas dentro de su jurisdicción. Para las PyMEs, pueden ser mejores las leyes de tecnología neutral que son más fáciles de cumplir y consideran las firmas electrónicas y las firmas manuales con la misma significancia legal. Aún así, una aplicación más clara de las leyes dentro de las jurisdicciones, particularmente aquellas con regímenes regulatorios más complejos, puede hacer una gran diferencia para facilitar las transacciones en línea.
- **Estructura institucional para los pagos electrónicos:** La creación de un solo organismo regulador o de aplicación podría ayudar a proporcionar un punto de contacto para la comunidad empresarial y facilitar la creación e implementación de normas y regulaciones. Algunos ejemplos de algunas jurisdicciones incluyen la creación de unidades especiales dentro de instituciones existentes o nuevos organismos o entidades regulatorias (esto puede incluir, por ejemplo, agentes de certificación terceros neutrales para las firmas electrónicas). La estructura institucional para los pagos electrónicos también debe tener en cuenta las normas internacionales y regionales para facilitarles a las empresas celebrar acuerdos transfronterizos.
- **Mejor aplicación de los marcos de pagos electrónicos:** También es un punto clave la aplicación adecuada de los marcos existentes de pagos electrónicos en todos los niveles (nacional, regional e internacional). Como en el caso de Sri Lanka, probablemente algunas jurisdicciones ya cuenten con leyes y regulaciones sólidas sobre los pagos electrónicos, pero que aún no se han aplicado eficazmente. La defensa puede enfocarse en una mayor colaboración y armonización entre las diferentes agencias de aplicación responsables de los pagos electrónicos y mayor cooperación internacional.
- **Adopción de marcos internacionales:** Una adopción e implementación más amplia de los marcos internacionales, como la Ley Modelo sobre Firmas Electrónicas de UNCITRAL – que se incorporó a las leyes nacionales en Latinoamérica – podría proporcionar una orientación regulatoria valiosa y promover la armonización de un enfoque tecnológicamente neutral que aborda mejor las necesidades de la comunidad empresarial global. Si bien las leyes modelo son pautas y no son "ley definida", aún así son trampolines para elaborar leyes nacionales aplicables. De manera alternativa, los elementos técnicos que se incluyen en la Ley Modelo de UNCITRAL pueden ayudar a las empresas a medida que involucran a organismos reguladores.

Lista de verificación para analizar las leyes y regulaciones existentes de firma electrónica y pago electrónico

¿Quién regula las transacciones electrónicas en línea en su jurisdicción (ministerio, organismo regulador, etc.)? ¿Hay un organismo o unidad reguladora dedicada para las transacciones electrónicas? ¿La misma entidad se centran en pagos electrónicos y firmas electrónicas?

¿Existen leyes, regulaciones y políticas que aborden específicamente los pagos electrónicos y firmas electrónicas, o se aplican en virtud de leyes de transacción financiera y de contrato más generales?

¿Qué tan flexible es el marco regulatorio cuando se trata de nuevos servicios innovadores de pagos electrónicos?

¿Su jurisdicción trata las formas bancarias de los pagos electrónicos de manera diferente de las formas no bancarias de los pagos electrónicos?

¿Su gobierno ha probado (o parecería estar dispuesto a probar) "Entornos Regulatorios de Prueba) que podrían permitir que las empresas experimenten y crezcan?

¿Qué enfoque toma su jurisdicción con respecto a las firmas electrónicas (tecnológicamente neutral, dos niveles o tecnológicamente específica)?

¿Existen desafíos administrativos o judiciales para las firmas electrónicas en su jurisdicción?

¿Existen vías existentes para el diálogo público y privado sobre las transacciones electrónicas? ¿Existen actualmente oportunidades para que el sector privado trabaje junto con organismos reguladores y responsables de formular políticas para crear y defender leyes sobre transacciones electrónicas?

¿Se notifica a las empresas cuando se está desarrollando un proyecto de ley y existe un proceso establecido para proporcionar comentarios?

¿Se ha involucrado con marcos que regulan las transacciones electrónicas en el nivel regional o internacional?

Usar el Análisis Profundo Legal

La Parte II de esta Guía contiene un Análisis Profundo Legal, que analiza de manera más detallada y comparativa las diferentes opciones regulatorias y enfoques dentro de cada una de las cuatro áreas de temas principales que se tratan aquí. La Guía sigue una metodología desarrollada por New Markets Lab (NML) para aumentar la concientización de los requisitos y derechos legales. Las Herramientas Legales de NML se han utilizado en todo el mundo como mecanismo para reunir a empresas y responsables de formular políticas para desarrollar un entendimiento compartido de cómo se pueden diseñar e implementar los sistemas regulatorios para generar un crecimiento económico inclusivo. Las Guías Legales de NML se basan en las necesidades de las partes interesadas y tienen un enfoque particular en las PyMEs y las partes interesadas económicas marginadas. Para identificar los temas principales en esta Guía, CIPE participó en la extensión y el diálogo continuos con sus socios locales del sector privado en todo el mundo.

Las Pautas Legales de NML no presentan consejo legal específico, que se debe buscar a través de un abogado certificado para practicar derecho en una jurisdicción específica, pero sí proporcionan una base de conocimiento sobre cuestiones legales y regulatorias generales, consideraciones comunes que afectan a las PyMEs y posibles enfoques para mejorar el diseño e implementación regulatorio. NML ha desarrollado Pautas Legales desde 2012, y ha acumulado una biblioteca de recursos enfocados en partes interesadas y regiones. En algunos casos, estas pautas se han utilizado para proporcionar un marco para defensa legal. En el nivel de país, NML también ha utilizado herramientas como Mapas de Sistemas Regulatorios para desglosar los procesos regulatorios complejos y orientar a las partes interesadas a través de una estrategia para identificar y priorizar puntos de intervención (similares a los temas que generan controversia, pero específicamente relacionados con los procesos regulatorios) que pueden conducir a una reforma sostenible. Todas las herramientas legales de NML están diseñadas para que los sistemas legales sean más transparentes, inclusivos y democráticos.

El Análisis Profundo Legal de la parte II de esta Guía no tiene la intención de ser prescriptivas, sino que detallan las disyuntivas regulatorias y legales y las perspectivas comerciales que se deben considerar para el desarrollo de un marco legal. Todos los sistemas legales son diferentes, y un marco bien adaptado a un sistema legal puede no funcionar de la misma manera para otro. Aún así, existen muchas lecciones para aprender para los responsables de elaborar políticas y la comunidad empresarial, que el enfoque comparativo de esta Guía propone resaltar.

El Análisis Profundo Legal también describe algunos modelos y marcos de ejemplo que existen en el nivel internacional y regional, que sirven como puntos de debate útiles para la comunidad empresarial. A menudo, los marcos y las iniciativas regionales y bilaterales contienen más detalle que los modelos en el nivel internacional, e incluyen ejemplos específicos de soluciones para los desafíos regulatorios comunes. Los organismos reguladores deben utilizar esta Guía para buscar ejemplos de enfoque innovadores y buenas prácticas emergentes. La comunidad empresarial puede utilizar la Guía para obtener un entendimiento más integral de las estructuras legales complejas que aplican a la economía digital para mejorar la implementación regulatoria y fortalecer un enfoque de defensa informado.

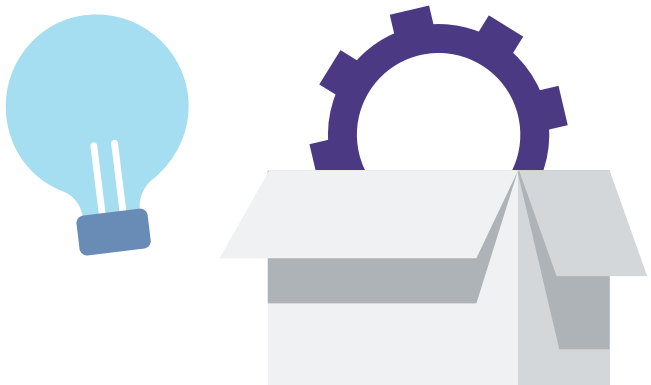
Un llamado a la acción

La naturaleza interconectada de la economía digital significa que los intereses y los riesgos de las empresas, consumidores, ciudadanos y representantes públicos se entrelazan profundamente. No hay economías digitales aisladas y nacionales, sino un conjunto de oportunidades y limitaciones nacionales para participar en el comercio digital internacional. Para algunos países y comunidades empresariales, la protección del consumidor, la protección de datos, la ciberseguridad y las transacciones electrónicas puede no parecer consideraciones legales o comerciales urgentes. Sin embargo, el crecimiento y desarrollo económico inclusivo depende de políticas y regulaciones nacionales que facilitan la competitividad en un mundo cada vez más digital. A medida que el alcance de la innovación digital se expande en todo el mundo, las empresas locales, especialmente en el Hemisferio Sur, enfrentará barreras excesivas para el ingreso y sostenibilidad, a menos que se preste atención a sus opiniones y participación en el diálogo y formulación de políticas.

Sin ninguna duda, la economía digital es difícil de abordar a través de políticas y regulaciones porque es un área muy técnica, en constante evolución y relativamente nueva del comercio global. No obstante, la reforma política democrática es posible cuando los argumentos persuasivos y bien razonados se respaldan con apoyo público y básico y un diálogo constructivo. Las campañas de defensa eficaces dependen de la credibilidad; es esencial establecer una reputación con el correr del tiempo desarrollando puentes entre sectores, promoviendo el interés público y participando en esfuerzos de reforma de políticas de manera transparente y abierta. Los grupos de defensa empresarial pueden abordar los temas de la economía digital identificando primero a los interesados con ideas similares, incluidas las empresas nuevas, universidades y organizaciones de sociedad civil con mentalidad tecnológica o miembros del gobierno. Las coaliciones de base amplia pueden garantizar canales productivos de diálogo con el público, los medios y responsables de elaborar políticas.

Las regulaciones efectivas y competitivas en la era digital deben promover innovación, crecimiento económico inclusivo y aumentar las oportunidades de inversión y colaboración tecnológica. Los beneficios de un mercado conectado y global pueden ya no pueden limitarse a un puñado de países y empresas multinacionales. La economía digital puede ser global, pero mejorar el entorno propicio para empresas en mercados emergentes y fronterizos implica que los agentes locales identifique recomendaciones de políticas personalizadas que faciliten su inclusión Al participar en el análisis y formación de las "reglas del juego" – los incentivos que definen la conducta económica y las cuestiones que afectan el desarrollo a largo plazo – las empresas pueden contribuir al diseño de una política pública inteligente que promueva el crecimiento y el acceso a la economía digital.

CIPE y NML esperan que las empresas y los gobiernos por igual aprovechen este llamado a la acción para fortalecer el entorno propicio para una economía digital sólida e inclusiva.



Recursos adicionales sobre defensa de políticas y guías legales

CIPE y NML recomiendan los recursos adicionales que se enumeran a continuación para ayudar a impulsar el largo y fructífero proceso de la reforma política democrática en la era digital:

- CIPE, How to Advocate Effectively: A Guidebook for Business Associations, 2007, https://www.cipe.org/resources/advocate-effectively-guidebook-business-associations/
- Kim E. Bettcher, Making the Most of Public-Private Dialogue: An Advocacy Approach, 2011, https://www.cipe.org/resources/making-public-private-dialogue-advocacy-approach/
- Kim E. Bettcher, Benjamin Herzberg, Anna Nadgrodkiewicz, Public-Private Dialogue: The Key to Good Governance and Development, 2015, https://www.cipe.org/resources/public-private-dialogue-key-good-governance-development/
- CIPE, Business Associations for the 21st Century http://www.cipe.org/vba/business-associations-guidebook
- CIPE, National Business Agenda Guidebook http://www.cipe.org/publications/detail/national-business-agenda-guidebook-voice-business
- New Markets Lab, East Africa Legal Guide, Aspen Network of Development Entrepreneurs, septiembre de 2016, https://docs.wixstatic.com/ugd/095963_54aad2211372409c89cba8790c279912.pdf
- New Markets Lab, Legal Guide for Women Entrepreneurs, Aspen Network of Development Entrepreneurs, actualización a partir de agosto de 2018.
- New Markets Lab, Legal Guide to Strengthen Tanzania's Seed and Inputs Markets, with USAID, AGRA, and SAGCOT, 2016, https://docs.wixstatic.com/ugd/095963_3a4f751a4c83488982341082f530aa32.pdf
- New Markets Lab, Working Draft, Transport Services Regulatory Guide, ICTSD, 2016.
- New Markets Lab, Working Draft, Tourism Services Regulatory Guide, ICTSD, 2016.
- New Markets Lab, Working Draft, Information and Communication Technology Services Regulatory Guide, ICTSD, 2016.
- New Markets Lab, Working Draft, Financial Services Regulatory Guide, ICTSD, 2016.

El proceso de diálogo, sus lecciones y los resultados ofrecen datos importantes para otros reformistas en otros países que trabajan para lograr una economía digital más inclusiva. CIPE alienta a aquellos que participan en diálogo y defensa sobre la economía digital y aquellos que usan esta Guía a compartir opiniones e historias con CIPE mediante tweets en @CIPEglobal **con el hashtag #DigitalEconomyDialogues.**

Abreviaciones y acrónimos

ADR	Resolución Alternativa de Disputas
AfCFTA	Zona de Libre Comercio de África Continental
APEC	Cooperación Económica de Asia-Pacífico
APEC CBPRs	Normas de Privacidad Transfronteriza de Cooperación Económica Asia-Pacífico
ASAPCP	Plan de Acción Estratégico para la Protección del Consumidor
ASEAN	Asociación de Naciones del Sudeste Asiático
CAUCA	Código Aduanero Unificado Centroamericano
CERT	Equipo de Respuesta para Emergencias Informáticas
CIPE	Centro para la Empresa Privada Internacional
CPTPP	Acuerdo Integral y Progresivo para la Asociación Transpacífica
CSF	Marco de Ciberseguridad
ECC-Net	Red Europeos de Centros del Consumidor
ECOWAS	Comunidad Económica de los Estados de África Occidental
eLAC2018	Agenda Digital para Latinoamérica y el Caribe 2018
ENISA	Agencia de la Unión Europea de Seguridad de las Redes y de la Información
eIDAS	Regulación sobre la Identificación Electrónica y los Servicios de Confianza para Transacciones Electrónicas en el Mercado Interno
EU BCR	Normas Corporativas Vinculantes de la Unión Europea
FTC	Comisión Federal de Comercio
GDPR	Regulación de Protección General de Datos
ICPEN	Red Internacional de Aplicación y Protección del Consumidor
ICT	Tecnología de la Información y las Comunicaciones
IEC	Comisión Internacional Electrotécnica
ISO	Organización Internacional de Normalización
MERCOSUR	Mercado Común del Sur
MPIW	Grupo de Trabajo de la Industria de Pagos Móviles
MSMR	Microminoristas, Minoristas Pequeños y Medianos
NAFTA	Tratado de Libre Comercio de América del Norte (TLCAN)
NIST	Instituto Nacional de Estándares y Tecnología
NML	New Markets Lab
OAS	Organización de los Estados Americanos
ODR	Resolución de Disputas En Línea

OECD	Organización para la Cooperación y el Desarrollo Económico
OSCE	Organización para la Seguridad y Cooperación en Europa
PCI DSS	Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago
PKI	Infraestructura de Claves Públicas
PSD2	Directiva de la Unión Europea sobre Pagos
PyMEs	Pequeñas y Medianas Empresas
TSP	Proveedor de Servicios de Confianza
UGC	Contenido Generado para el Usuario
RU	Reino Unido
UNCITRAL	Comisión de las Naciones Unidas sobre la Ley de Comercio Internacional
UNGCP	Pautas de las Naciones Unidas para la Protección del Consumidor
EE. UU.	Estados Unidos
US	Estados Unidos
WTO	Organización Mundial del Comercio

Glosario

Análisis de datos: uso extensivo de datos para mejorar las predicciones y apoyar la toma de decisiones

Arbitraje: una forma de resolución alternativa de disputas por la cual las partes acuerdan designar a un tercero independiente (un tribunal compuesto de uno o más árbitros) para resolver la disputa entre ellos y acuerdan que la decisión será vinculante

Cláusula de extraterritorialidad: una disposición legal que permite la aplicación de leyes nacionales a empresas de comercio electrónico en el extranjero

Criptomonedas: una moneda digital o virtual que utiliza técnicas de encriptado para la seguridad y generalmente opera sin un banco central

Derecho a acceso: el derecho de los sujetos de los datos a acceder a sus datos personales e información complementaria

Derecho a rectificación: el derecho de los sujetos de los datos a corregir o completar datos personales inexactos o incompletos sin demora excesiva

Derecho a ser informado: el derecho de los sujetos de los datos a ser informados sobre la recopilación y uso de sus datos personales

Derecho a portabilidad de datos: el derecho de los sujetos de los datos a obtener y reutilizar los datos personales para sus propios fines en diferentes servicios

Derecho a eliminar: el derecho de los sujetos de los datos a eliminar sus datos personales

Derecho a oponerse: el derecho de los sujetos de los datos a oponerse a marketing directo o procesamiento

Derecho a restricción de procesamiento: el derecho de los sujetos de los datos a solicitar la restricción de supresión de sus datos personales

Derecho a revocar (o período de reflexión): el derecho de los consumidores a cancelar un pedido en línea dentro de un plazo de tiempo predeterminado

El Referencial: un medio para facilitar las certificaciones duales para la transferencia de datos bajo mecanismos de transferencia de datos de la Unión Europea y Normas de Privacidad Transfronteriza de Cooperación Económica Asia-Pacífico

Enfoque basado en riesgos: una estrategia de monitoreo de ciberseguridad que requiere que entidades públicas y privadas realicen evaluaciones regulares de riesgos y procesos de monitoreo, evalúen periódicamente la eficacia de los controles identificados y ajusten sus mecanismos de control sobre la base de su evaluación

Enfoque de adecuación: evaluación de la adecuación de las leyes y regulaciones de una jurisdicción (en esta Guía, se utiliza para referirse a una base para permitir la transferencia transfronteriza continua de datos en donde los organismos reguladores evalúan si las leyes nacionales de la jurisdicción que exporta los datos son adecuadas para proteger la transferencia)

Enfoque de normas corporativas vinculantes: una base para permitir la transferencia transfronteriza continua de datos mediante la cual los organismos reguladores evalúan si los mecanismos de revisión independiente de una empresa son suficientes

Firmas de clic para firmar: un tipo de firma electrónica que incluye marcar casilleros, e-squiggle y nombres tipeados

Firmas digitales: el tipo de firma más avanzado y seguro, que utiliza una identificación digital basada en certificado emitida por una Autoridad de Certificación o Proveedor de Servicios de Confianza (TSP) que vincula de forma única la firma a la identidad del firmante

Forum Shopping: cuando una parte de una disputa reconoce que múltiples tribunales pueden tener jurisdicción sobre el reclamo y elige uno que tratará su reclamo más favorablemente

Facilitación del comercio: la simplificación, modernización y armonización de procesos de exportación e importación para el comercio de bienes

Firmas electrónicas básicas: un tipo de firma electrónica donde el firmante aplica su firma manual a un documento de manera electrónica y el documento en general está protegido con una firma digital criptográfica propiedad de una organización proveedora de servicios que actúa como "testigo" de la firma

Infraestructura de claves públicas: un medio de autenticación y control de acceso a redes no confiables como redes de telecomunicaciones abiertas o internet; en general, se utilizan para verificar firmas digitales

Jurisdicción: un país, estado u otra área donde se debe obedecer un determinado conjunto de leyes o normas; las jurisdicciones pueden ser países o naciones, entidades subnacionales, uniones económicas (por ejemplo, la Unión Europea) o territorios autónomos (por ejemplo, Hong Kong). Las jurisdicciones se pueden superponer dentro de un territorio.

Leyes medidas legales que generalmente deben atravesar un proceso parlamentario, que crean un marco para regir el mercado y, a menudo, se relacionan con un determinado sector o actividad. Las leyes tienden a ser más generales que las regulaciones y crean obligaciones legalmente aplicables.

Mediación: una forma de resolución alternativa de disputas donde un tercero independiente (mediador) utiliza la persuasión en lugar del poder legal para llegar a una resolución

Pagos de la Cámara de Compensación Automatizada: un sistema electrónico de transferencia de fondos

Pagos electrónicos bancarios: pagos electrónicos que se conectan a los sistemas bancarios a través de diferentes tipos de cuentas bancarias, como tarjetas de débito, tarjetas de crédito y Pagos de la Cámara de Compensación Automatizada

Pagos electrónicos no bancarios: pagos electrónicos no conectados a sistemas bancarios

Políticas: principios o estrategias que guían las acciones gubernamentales (y pueden contener objetivos para leyes y regulaciones), pero no tienden a ser instrumentos legalmente vinculantes por sí solas

Requisito de localización de datos: el requisito que indica que las empresas deben almacenar datos o una copia de los datos en servidores físicamente ubicados dentro de las fronteras nacionales

Resolución alternativa de disputas: un mecanismo para resolver disputas por el cual las partes utilizan técnicas que no son litigios para llegar a un acuerdo

Regulación ex ante: regulaciones que contienen requisitos para ingresar y operar en el mercado a través de una aprobación regulatoria según el caso o medidas más amplias (en esta Guía, se refiere a la regulación de pagos electrónicos no bancarios)

Regulación ex post: regulaciones que se aplican una vez que las empresas están operando en el mercado (en esta Guía, se refiere a la regulación de pagos electrónicos no bancarios)

Regulaciones no prudenciales: regulaciones financieras que se aplican a cuestiones que no sean la estabilidad del sistema financiero o las instituciones individuales; cubre todas las regulaciones financieras que no son macro prudenciales (relacionadas con la estabilidad del sistema financiero) o micro prudenciales (relacionadas con la estabilidad de las instituciones financieras individuales)

Regulación prescriptiva(o regulación específica de tecnología): regulaciones que especifican un determinado método o tecnología; en esta guía se utiliza para referirse a las regulaciones de firmas electrónicas que legalizan tipos limitados de firmas electrónicas

Regulación prudencial (o regulación micro prudencial): regulaciones financieras que se relacionan con la estabilidad de instituciones financieras individuales

Regulaciones: medidas legales que se crean, generalmente a través de acción administrativa, para implementar leyes; tienden a ser más detalladas que las leyes y también más fáciles de cambiar

Regulación financiera (o regulación macro prudencial): regulaciones financieras que cubren un rango de medidas diseñadas para identificar y mitigar riesgos para la estabilidad del sistema financiero en general

Regulación tecnológicamente neutral: regulaciones que se aplican sin importar el tipo de tecnología subyacente; en esta guía, el término se refiere a 1) las regulaciones sobre firmas electrónicas que se aplican de igual manera a las firmas manuales y firmas electrónicas (sin importar las tecnologías de autenticación subyacentes) y 2) leyes y regulaciones de protección del consumidor que se aplican en la economía digital y tradicional

Regulación de dos niveles: regulaciones sobre firmas electrónicas que reconocen la legalidad y validez de múltiples tipos de firmas electrónicas, pero que dan un mayor valor probatorio a las firmas digitales autenticadas por ciertas tecnologías

Sujetos de los datos: personas cuyos datos personales se recopilan, mantienen o procesan

Tecnología regulatoria: una nueva categoría de negocios que usan análisis de datos para ayudar a las empresas a cumplir con las regulaciones; principalmente para cumplir con regulaciones financieras

Tribunales para reclamos menores: procesos judiciales especiales para manejar reclamos bajo un umbral monetario específico que generalmente son más rápidos y menos costosos

Parte II – Análisis Profundo Legal

Análisis Profundo Legal – Protección del consumidor

La ley de protección del consumidor es esencial para todas las transacciones, ya que protege a las personas y empresas que compran bienes y servicios a través de medios electrónicos y no electrónicos. Las leyes de protección del consumidor pretenden proteger a los consumidores de "bienes y servicios descriptos incorrectamente, dañados, fallados y peligrosos, y de prácticas comerciales y crediticias injustas[1]". Tradicionalmente, los marcos legales para la protección del consumidor han sido diseñadas para abordar las necesidades de los clientes en un entorno fuera de línea. No obstante, la protección del consumidor es sin duda importante en la economía digital. Las protecciones adecuadas ayudan a cultivar un entorno confiable para que los consumidores y las empresas locales puedan realizar de manera segura transacciones en línea. En la actualidad, los regímenes convencionales de protección del consumidor, en general, no están equipados para abordar prácticas relativas al comercio electrónico, como la publicidad en redes sociales. Como resultado, existen brechas en la protección del consumidor en la mayoría de los sistemas legales, y las comunidades empresariales locales consideran que sus necesidades particulares no están bien atendidas.

Este análisis profundo de los marcos legales y regulatorios que rigen la protección del consumidor en línea presenta algunos ejemplos ilustrativos de las diferentes prácticas regulatorias relacionadas con la economía digital. También aborda las consideraciones clave para la comunidad empresarial local y los organismos reguladores a medida que más países comienzan a promulgar e implementar marcos de protección del consumidor que abordan específicamente cuestiones del consumidor digital. Este análisis profundo comienza con una descripción general de los marcos internacionales y regionales ya implementados para la protección del consumidor, que es un punto de partida útil para los diálogos sobre política en el nivel nacional. Luego describe algunos enfoques regulatorios comunes con respecto a la protección del consumidor, los desafíos específicos relacionados con la implementación y aplicación de regulaciones y ejemplos de marcos institucionales relevantes. Además, la sección de Protección del consumidor en la Guía Resumida contiene información sobre orientación empresarial y de defensa para la comunidad empresarial local, incluso una lista de verificación para analizar las leyes y regulaciones locales de protección del consumidor existentes.

Marco internacional y regional para la protección del consumidor

Las pautas internacionales son útiles para identificar los derechos y preocupaciones de los consumidores y las empresas. Son áreas donde pueden ser necesarias nuevas regulaciones o reformas a las regulaciones existentes. En segundo lugar, un marco internacional podría ayudar a promover la cooperación entre gobiernos, mejorar la aplicación y permitir una exploración en colaboración de maneras para superar los desafíos comunes en el sector. Fundamentalmente, las iniciativas regionales contienen disposiciones más detalladas que las de nivel internacional, y brindan puntos de intervención más específicos para los esfuerzos de defensa. La Tabla 1 presenta algunas iniciativas internacionales y regionales ilustrativas actuales para la protección del consumidor.

Tabla 1. Marco internacional y regional para la protección del consumidor

Iniciativas	Implicaciones para la comunidad empresarial
Multilateral	
• Las Pautas de la Organización para la Cooperación y el Desarrollo Económico (OECD) para la protección del consumidor en el comercio electrónico[2] • La Pauta de las Naciones Unidas para la Protección del Consumidor (UNGCP)[3] • La ley modelo de la Comisión de las Naciones Unidas sobre la Ley de Comercio Internacional (UNCITRAL) sobre el comercio electrónico[4] • La Red Internacional de Aplicación y Protección del Consumidor (ICPEN)[5]	• En general, las iniciativas en el nivel multilateral promueven la cooperación y el intercambio de información, pero no establecen un marco internacional unificado para la protección del consumidor. Esta es una posible vía para futuras participaciones. Si bien pueden asistir a las comunidades empresariales locales en el contexto de elaboración de políticas nacionales, los marcos internacionales son más detallados en otras áreas en cuestión. • Las pautas de OECD cubren las transacciones entre consumidores (no solo entre empresas y consumidores), por lo tanto, cubren un amplio rango de partes interesadas en la economía digital. Las pautas de OECD se centran en la cooperación y coordinación entre las autoridades de aplicación de protección del consumidor para mejorar la eficacia de las investigaciones activas. • Si bien la Ley Modelo de UNCITRAL menciona la protección del consumidor. no contiene obligaciones específicas del país. Brinda una perspectiva más general de cómo la protección del consumidor se aplica al comercio internacional. • La OECD, UNGCP e ICPEN facilitan o promueven la cooperación multinacional y el intercambio de información. Alivia la carga que cae en la comunidad empresarial de investigar las regulaciones superpuestas.

	• La ICPEN facilita el intercambio de información; publica pautas que promueven la transparencia; y sirve como sitio de reclamo por estafas en línea. La comunidad empresarial podría usar esta red como un foro neutral para resolver disputas, y como fuente confiable de información sobre las leyes de protección del consumidor.
Regional	
• Nuevo Marco de Cooperación de Protección del Consumidor (CPC, por sus siglas en inglés) (2017)[6] • Red Europea de Centros del Consumidor (ECC-Net)[7] • El Plan de Acción Estratégico para la Protección del Consumidor (ASAPCP) de la Asociación de Naciones del Sudeste Asiático (ASEAN)[8] • Agenda Digital para Latinoamérica y el Caribe (eLAC2018)	• Las iniciativas regionales que se centran en la protección del consumidor contienen ejemplos de buenas prácticas regulatorias que se podrían adaptar a nivel nacional. Estos canales también podrían ser utilizados en mayor medida por grupos empresariales dentro de las regiones relevantes. • El marco de CPC facilita la aplicación de normas regionales del consumidor, específicamente para las transacciones transfronterizas. • La ECC-Net sirve como un centro asesor regional para los derechos y obligaciones de protección del consumidor. Con mecanismos de apoyo integrados para las partes interesadas para el sector público y privado, como municipios de la comunidad y reuniones de alineación de partes interesadas, la ECC-Net actúa como una vía para la defensa en el nivel europeo. • El ASAPCP integra las políticas de protección del consumidor de ASEAN y establece una red regional de resolución de disputas en línea (ODR). Forma un canal de aplicación adicional dentro de los estados miembro de la ASEAN. • La eLAC2018 pretende adaptar regulaciones de protección del consumidor existentes al entorno digital en toda la región. También proporciona vías para la participación del sector privado en el proceso de toma de decisiones.

Enfoques regulatorios para la protección del consumidor

Los marcos regulatorios de protección del consumidor varían considerablemente de país en país. No obstante, todos los marcos apuntan a lograr un equilibrio entre los derechos y las responsabilidades de todas las partes interesadas en una transacción electrónica. Para entender mejor esos derechos y obligaciones legales, las empresas locales primero deben entender dónde residen las responsabilidades de protección del consumidor. La responsabilidad tiende a ser asignada entre organismos reguladores, consumidores y la industria, particularmente plataformas de comercio electrónico y proveedores en línea. Las responsabilidades se asignan de manera diferente en cada etapa de una transacción: etapa previa a la compra, pago y posterior a la venta o entrega. Entender las normas en cada etapa ayudará a los defensores de la comunidad empresarial local a tomar decisiones informadas sobre las disyuntivas que existen dentro de cada enfoque regulatorio.

Para la asignación de responsabilidades, algunos países (como Chile y los EE. UU.[9]) dependen enormemente del sistema judicial. En estos lugares, los métodos adecuados de resolución de disputas son de gran importancia. Otras jurisdicciones se centran más en la regulación gubernamental o la autorregulación empresarial; algunas trabajan para empoderar a los consumidores con información, para que puedan tomar decisiones informadas para impulsar el mercado[10]. Las asociaciones públicas-privadas son un mecanismo popular para el feedback. En España, por ejemplo, las empresas pueden optar por registrarse voluntariamente y cumplir con el Código Ético de Confianza Online, orientado a la publicidad, las transacciones de comercio electrónico y los mecanismos de reparación para el consumidor. Esto los obliga a cierto estándar de cuidado, que se actualiza frecuentemente para reflejar los cambios de la ley.[11] Otros países, como Malasia, regulan específicamente empresas anfitrionas que operan a través de modelos comerciales basados en una plataforma.[12]

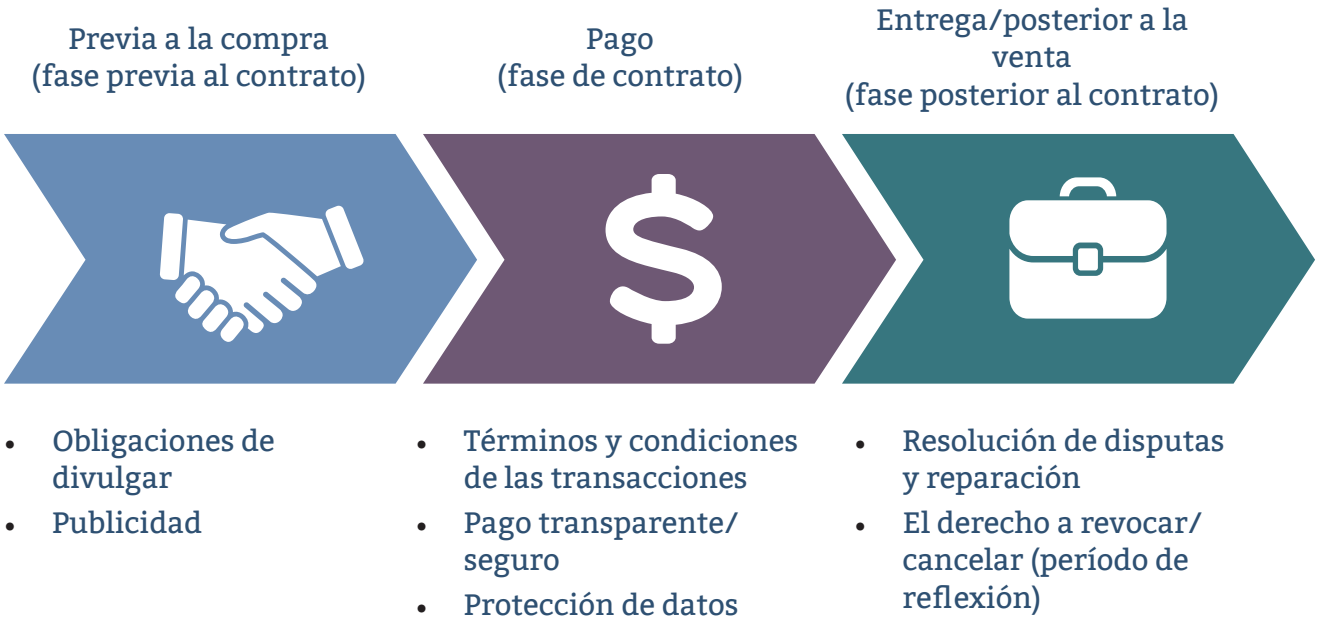
Muchas jurisdicciones cuentan con leyes, regulaciones o políticas de protección del consumidor que aplican a transacciones tradicionales fuera de línea. Algunos eligen aplicar estas mismas leyes a la economía digital, ya que abordan las necesidades del consumidor presenten en las transacciones en línea y fuera de línea. Otros han elegido crear leyes o regulaciones completamente nuevas para abordar las necesidades especiales de la economía digital. Un buen ejemplo es la Ley de Protección del Consumidor en el Comercio Electrónico de Corea del Sur.[13]

La comunidad empresarial local siempre debe asegurarse de identificar los aspectos del comercio electrónico que no están cubierto por el régimen regulatorio existente: falsificación de bienes, por ejemplo, o publicidad en las redes sociales.

Los regímenes de protección del consumidor con frecuencia comparten algunos elementos en común. Estos elementos en común abordan las necesidades del consumidor en diferentes etapas de una transacción, como se muestra en el **Diagrama 1**. (Esta Guía aborda dos de esos elementos, la protección de datos y pagos en línea transparentes y autenticados, en capítulos posteriores.) Las comunidades empresariales locales se benefician de un régimen de protección que aborda cuestiones a lo largo de las diferentes etapas de la transacción; desarrolla confianza en el comercio electrónico, simplifica las transacciones digitales e involucra a más consumidores en línea.

El resto de esta sección ilustra las maneras en que las diferentes jurisdicciones abordan cada elemento de la protección de los consumidores en una determinada transacción.

Diagrama 1. Elementos regulatorios de la protección del consumidor



Fuente: New Markets Lab (2018)

Obligaciones de divulgar: Muchas jurisdicciones designan los tipo de información que los proveedores en línea deben divulgar para que los consumidores puedan realizar compras informadas. Esta información en general se clasifica como 1) **información comercial**, como el nombre del comerciante y la dirección donde el comerciales está establecido, conforme a lo requerido en la Unión Europea (EU);[14] 2) **etiquetado obligatorio de productos**, particularmente para los productos de alto riesgo como los alimentos; y 3) divulgación de los resultados de inspección del gobierno.[15]

Los defensores de la comunidad empresarial local deben conocer las maneras en que los organismos reguladores asignan el riesgo dentro de su jurisdicción, y qué obligaciones se imponen para las empresas en lugar de los consumidores.

Publicidad: Las publicidades son representaciones realizadas por vendedores para informar y atraer a consumidores a un producto o servicio. Las leyes de protección del consumidor asegurar que dichas representaciones no sean engañosas.[16] Un área de gran importancia aquí es si las regulaciones de publicidad convencionales aplican en línea. En muchas jurisdicciones, como Japón,[17] las leyes de publicidad existentes también aplican en línea en los mercados y son regidas por las mismas autoridades reguladoras. El aumento de la publicidad en las redes sociales también ha planteado algunas cuestiones legales interesantes. Algunas jurisdicciones han promulgado regulaciones que van mucho más allá de los proveedores tradicionales de comercio electrónico. Por ejemplo, la Autoridad de Estándares de Publicidad de Singapur emitió pautas que requieren que los anunciantes, incluso celebridades (o "influencers"), deben divulgar completamente en lenguaje sencillo sus relaciones con las marcas cuando promocionan o respaldan productos a través de las redes sociales.[18] Otra táctica reciente es el contenido generado

por el usuario (UGC, por sus siglas en inglés), incluso revisiones y clasificaciones del consumidor en línea sobre sitios web como Yelp y TripAdvisor. Las cuestiones legales comunes que se relacionan con UGC incluyen propiedad intelectual, privacidad de los datos y consentimiento.[19]

Términos y condiciones de las transacciones: Como cualquier transacción, las ventas digitales tienen ciertos términos y condiciones que tienen implicaciones de protección del consumidor. Los aspectos más relevantes son 1) **la divulgación y transparencia**, y 2) **términos y condiciones justas**. Estos van de la mano porque las normas de divulgación y transparencia obligan a los comerciantes a exhibir los términos y condiciones que "probablemente afecten la decisión de un consumidor con respecto a una transacción".[20] La divulgación también debe ser accesible. Por ejemplo, en Argentina, los comerciales deben proporcionar acceso claro, completo e inequívoco a los términos generales.[21] En la práctica, los términos y condiciones pueden ser difíciles de comprender para los consumidores, lo que puede perjudicar la intención. Un análisis del Reino Unido (RU) indicó que el 43 por ciento de los adultos en Inglaterra no podían entender los términos y condiciones de 2013 de Google.[22] Sin embargo, hay pocas regulaciones que rigen el uso de un lenguaje claro y comprensible para todos.

Las empresas podrían seguir la recomendación de la OECD de que la divulgación en línea y sus términos se realicen en un "lenguaje sencillo y fácil de entender".[23] La comunidad empresarial y las autoridades reguladoras también podrían ir un paso más allá y promover que las divulgaciones se realicen en múltiples idiomas locales. Si bien esto podrían imponer una mayor carga para las pequeñas y medianas empresas (PyMEs) y las empresas nuevas, promovería la diversidad. La "imparcialidad" se interpreta de manera diferente en las jurisdicciones. Si bien algunas jurisdicciones siempre respetan los contratos estándar entre corporaciones y consumidores, otros (como la UE) consideran que un término que no ha sido negociado individualmente (como los que aparecen con frecuencia en los contratos estándar) es injusto si perjudica el equilibrio entre los derechos y obligaciones de las partes.[24] Al promover una definición más armonizada de imparcialidad, las comunidades empresariales locales pueden ejercer sus derechos con respecto a este tema.

Resolución de disputas y reparación: Las disputas entre comerciantes y consumidores surgen con regularidad en el comercio electrónico. Existen diferentes mecanismos para resolver estas disputas, cada uno con sus propias disyuntivas y particularidades. Los sistemas judiciales tradicionales no siempre son confiables. Son un foro notablemente difícil para que los consumidores hagan cumplir los derechos en línea debido a los costos judiciales, acceso limitado a abogados adecuados, complicaciones sobre los límites de jurisdicción, y un trabajo de litigación extenso que actúa en contra del consumidor.[25] Para las transacciones del comercio electrónico, la resolución de disputas en línea (ODR), que ofrecen entidades públicas y privadas, puede ser una alternativa más rápida que un tribunal.[26] El arbitraje y la mediación también son otras opciones.

La mejor opción en una disputa determinada dependerá de la confiabilidad del sistema judicial local; la disponibilidad de árbitros calificados y asequibles; la confidencialidad de las sentencias, que generalmente se preservan en el arbitraje; y la habilidad de apelar una decisión (los resultados de un panel de arbitraje solo se pueden apelar en circunstancias limitadas).[27] En el caso de disputas contractuales entre jurisdicciones, el arbitraje tiende a tratar a las partes extranjeras con mayor neutralidad. A nivel nacional, el

arbitraje generalmente funciona mejor que el litigio en un tribunal,[28] aunque puede ser costoso para los consumidores y pequeñas empresas.

Trabajar junto con el sector público para diseñar mecanismos de resolución de disputas justos y equitativos es una buena manera para que la comunidad empresarial proteja sus derechos.

Derecho a revocar/cancelar (período de reflexión): Como es más difícil inspeccionar productos antes de la compra en el comercio electrónico, los consumidores son vulnerables al marketing engañoso. Como resultado, algunos organismos reguladores han intervenido para proporcionar a los consumidores el derecho a cancelar sus pedidos, llamado el derecho a revocar o el período de reflexión. La duración de este período varía: 14 días en la UE,[29] 7 días en China,[30] 5 días en Singapur y 10 días en Malasia.[31] Algunos organismos reguladores también han impuesto un precio mínimo, y por debajo de ese precio no se puede ejercer el derecho a revocar. En los Estados Unidos, por ejemplo, ese precio el $25 en el nivel federal. Algunas jurisdicciones también incluyen excepciones al derecho a revocar: los bienes personalizados, las mercaderías perecederas o el contenido digital están exentos de la norma del derecho a revocar.[32] Las regulaciones claras sobre los derechos a revocar podrían ayudar a proteger tanto a los consumidores como a la comunidad empresarial local reduciendo la cantidad de disputas. Esto, a la vez, podría aliviar los tribunales de una parte de su carga.

Implementación y aplicación de la protección del consumidor

A medida que las transacciones comerciales se vuelven cada vez más internacionales, la aplicación sigue siendo local. Existen desafíos para todas las partes interesadas que buscan la aplicación adecuada de las leyes de protección del consumidor. Al igual que la publicidad adecuada y la divulgación de los términos y condiciones, el lenguaje y las diferencias culturales complican la implementación y aplicación. Lo que las personas entienden en un contexto de mercado local o regional no necesariamente se traducirá al mercado global. Incluso la traducción de plataformas en línea puede causar problemas, especialmente para las industrias sin estándares y terminología en común. No todas las compañías tienen la capacidad de traducir una página web en el idioma de los consumidores, o anticipar por completo las necesidades de los consumidores. Además, muchos consumidores no saben dónde presentar quejas en una disputa internacional.

Para la aplicación de la ley y los procesos jurídico, hacer que las partes acuerden la traducción de un documento determinado (como los términos y condiciones de las transacciones) puede ser costoso y llevar mucho tiempo. El grado en que los funcionarios de aplicación de la ley cooperan entre jurisdicciones puede obstaculizar la buena aplicación. A pesar de estos desafíos, hay amplias oportunidades para que la comunidad empresarial local se involucre en los esfuerzos que apoyarían mejor la implementación de las leyes. El estudio de caso sobre ODR en Perú de la Guía Resumida proporciona un ejemplo de cooperación entre el sector público y privado para mejorar la aplicación. También demuestra cómo la comunidad empresarial local puede trabajar de manera proactiva para resolver algunos de estos desafíos regulatorios clave.[33]

Marcos institucionales relacionados con la protección del consumidor

Como con la aplicación y la implementación, un desafío principal dentro del marco institucional de la protección del consumidor es una designación clara de la autoridad. En muchas jurisdicciones, un organismo regulador central o ministerio, con amplia autoridad legislativa y de supervisión, maneja la protección del consumidor.[34] Este enfoque centralizado puede minimizar la superposición de mandatos regulatorios, mantener la consistencia de las políticas, y reducir conflictos potenciales entre las diferentes agencias.[35] Algunos ejemplos de este enfoque incluyen la Institución danesa del Defensor del Consumidor; el Ministerio de Industria, Inversión, Comercio y Economía Digital en Marruecos; y la Comisión Nacional del Consumidor en Sudáfrica. Notablemente, debido al estrecho vínculo entre la política de competencia y la protección del consumidor,[36] algunos organismos reguladores de protección del consumir también son organismos reguladores de competencia.[37]

Algunas jurisdicciones han adoptado un enfoque más sectorial, que puede permitir que los organismos reguladores desarrollen una experiencia más profunda en su industria regulada y responder a las necesidades regulatorias específicas de la industria. Australia y Noruega siguen este modelo.[38] Sin importar el enfoque que se utiliza, una consideración clave compartida para la comunidad empresarial local es la claridad con respecto a las responsabilidades y tareas específicas que cada organismo regulador tiene.

Análisis Profundo Legal – Protección de datos

A veces llamados el aceite de la economía digital, los datos se han convertido en un producto global clave y se utilizan, procesan, intercambian y analizan en cantidades masivas para potenciar el contenido, los bienes y los servicios digitalizados. Las regulaciones de protección de datos se relacionan con las personas que compran bienes y servicio electrónicamente y las compañías que compran, vender o brindan servicios en línea protegiendo los datos que se envían en estas transacciones.

La regulación tiende a seguir los pasos del ciclo de vida de los datos: recopilación y procesamiento de datos, almacenamiento, transferencia y eliminación. Sin embargo, las empresas pueden tener diferentes consideraciones con respecto a cómo se deben regular los datos, dependiendo de su modelo empresarial específico.

Este análisis profundo de los marcos legales y regulatorios que rigen la protección de datos en línea presenta algunos ejemplos ilustrativos de las diferentes prácticas regulatorias que se utilizan en todo el mundo. También aborda las consideraciones clave para la comunidad empresarial local y los organismos reguladores a medida que más países comienzan a promulgar e implementar marcos de protección de datos. El análisis profundo comienza con una descripción general de los mercados internacionales y regionales que ya existen. Luego describe algunos enfoques regulatorios comunes con respecto a la protección de datos, incluso marcos institucionales y desafíos específicos relacionados con la implementación y aplicación. Además, la sección de Protección de datos en la Guía Resumida contiene orientación empresarial y de defensa para la comunidad empresarial local, incluso una lista de verificación para analizar las leyes y regulaciones locales de protección de datos existentes.

Marco internacional y regional para la protección de datos

Los marcos legales para la protección de datos difieren de país en país, lo que dificulta entender las normas cuando se trabaja en múltiples mercados. Las compañías que dependen de las importaciones y exportaciones de datos a menudo enfrentan costos de cumplimiento y una incapacidad de operar en ciertos mercados. Existen iniciativas internacionales para armonizar los marcos nacionales en curso; hasta ahora, estas iniciativas solo han establecido principios generales.

Las normas en el nivel regional tienden a ser más claras, pero aún carecen de una armonización general. Las comunidades regionales también han comenzado a trabajar en colaboración para simplificar las normas sobre la protección de datos. Por ejemplo, la Cooperación Económica de Asia-Pacífico (APEC) y la UE ya han tomado medidas para facilitar las certificaciones duales, incluso la aprobación de un acuerdo referencial en 2014.[39] Este sistema de certificación ha recibido el apoyo de los organismos reguladores y grupos de defensa empresarial por igual (consulte el estudio de caso a continuación). Si bien no está claro si este programa se iniciará oficialmente, ni cuándo, parece que la certificación de APEC acelerará y reducirá el costo de la certificación en virtud de las Normas Corporativas Vinculantes de la Unión Europea (EU BCR).[40] Este esfuerzo de vincular sistemas regionales podría ser un buen modelo para la colaboración interregional.

Las comunidades empresariales locales pueden exigir activamente a los gobiernos que faciliten el flujo de datos transfronterizos. Esto se puede hacer a través de una coalición de asociaciones empresariales en diferentes jurisdicciones, como lo demuestra la expansión de las Normas de Privacidad Transfronteriza (CBPR) de la APEC. El Marco de Privacidad de la APEC fue creado para promover un grupo común de normas y estándares de protección de datos para facilitar la transferencia transfronteriza de datos en Asia y el Pacífico. Establece un marco único de principios y pautas de implementación (por ejemplo, protecciones de la seguridad) y permite a sus 21 miembros adoptar el Marco de Privacidad, con flexibilidad en la forma de hacerlo. Las compañías que trabajan en países de APEC pueden ser proactivas y certificar que cumplen con el Marco de Privacidad de la APEC adoptando las Normas de Privacidad Transfronteriza de la APEC (APEC CBPR), respaldadas por líderes de la APEC en 2011. APEC CBPR son normas voluntarias pero aplicables para la transferencia transfronteriza de datos, y están respaldadas ampliamente por la comunidad empresarial APEC CBPR pueden ser particularmente útiles para las empresas locales que dependen de la transferencia transfronteriza de datos, pero que no cuentan con recursos para formular sus propios programas de privacidad; como es el caso de las economías de la Asociación de Naciones del Sudeste Asiático (ASEAN), donde las PyMEs comprende el 96 por ciento de todas las empresas.

A fines de 2016, ocho grupos empresariales importantes que representan miles de empresas en todo el mundo publicaron conjuntamente una declaración que expresaba su apoyo del sistema de CBPR y que convocaba a 21 miembros de la APEC a aumentar la participación en CBPR para los estados miembro y el sector privado. Esta defensa ha tenido un impacto, ya que ahora seis economías participan en el programa de CBPR, y se espera que se unan más.

Estudio de caso:
Marco de privacidad de Cooperación Económica de Asia-Pacífico (APEC)

Los acuerdos de comercio también fortalecen el vínculo entre las cuestiones del comercio internacional y la economía digital, incluso la protección de datos.[41] A diferencia de las iniciativas específicas de privacidad, los acuerdos de comercio no imponen obligaciones positivas significativas. En cambio, apuntan a crear un equilibrio entre las leyes de protección de datos y las consideraciones de comercio. Estados Unidos ha defendido este enfoque, y rápidamente se está convirtiendo en un estándar, como lo demuestra el Tratado de Libre Comercio entre EE. UU. y Corea del Sur, el Acuerdo Integral y Progresivo para la Asociación Transpacífica (CPTPP) (el acuerdo de seguimiento de la Asociación Transpacífica),[42] y el reciente Acuerdo de libre comercio entre Singapur y Sri Lanka.[43] Incluir las disposiciones de datos dentro de los acuerdos de comercio podría limitar el grado en que las naciones individuales pueden abordar la protección de datos, y puede requerir que los gobiernos equilibren un amplio rango de áreas de políticas difícil de manejar, como la protección ambiental y la reducción de tarifas. La **Tabla 2** a continuación resume los instrumentos importantes globales, regionales y bilaterales aplicables a la protección de datos.

Fuente: CPBRs, About the APEC CBPR System. Web; ITI, Global Industry Groups Call for APEC Leadership on Facilitating Cross-Border Flows of Information with High Standards of Privacy Protection. Web. 18 de noviembre de 2016

Tabla 2. Marco internacional y regional para la protección de datos

Marco	Implicaciones para la comunidad empresarial
Multilateral	
• Las Pautas de OECD sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales[44] • Convención para la protección de individuos con respecto al procesamiento automático de datos personales[45]	• Las Pautas de OECD proporcionan ocho principios y conceptos con amplio apoyo internacional (por ejemplo, evaluación de riesgos y mayor interoperabilidad) Son un excelente recurso para las comunidades empresariales locales y los organismos reguladores por igual.
Regional	
• CPTPP[46] • APEC[47] • Convención de la Unión Africana sobre la Ciberseguridad y la Protección de Datos Personales[48] • Ley Complementaria sobre la Protección de Datos de la Comunidad Económica de los Estados de África Occidental (ECOWAS)[49] • Tratado de Libre Comercio de América del Norte (TLCAN) (en renegociación)[50]	• Los marcos regionales de protección de datos resaltan posiciones regulatorias ilustrativas y detalles de sus disposiciones. Estos canales también podrían ser utilizados en mayor medida por grupos empresariales dentro de las regiones relevantes. • Todos los acuerdos regionales en esta lista abordan la protección de datos específicamente. • La APEC, por ejemplo, permite que las compañías obtengan certificación para demostrar el cumplimiento con el Marco de Privacidad de APEC a través de un mecanismo voluntario, lo que es una buena práctica para una autorregulación más sólida. También establece principios y pautas de implementación para facilitar la transferencia de datos y enfoques armonizados entre los miembros de la APEC.
Bilateral	
• Tratado de Libre Comercio entre EE. UU. y Corea del Sur[51]	• Los acuerdos de comercio bilaterales están comenzando a contener disposiciones relacionadas directamente con los flujos de información electrónica, como se destaca en este ejemplo, que podrían informar las posiciones adoptadas por la comunidad empresarial a nivel nacional y con respecto a futuros acuerdos.

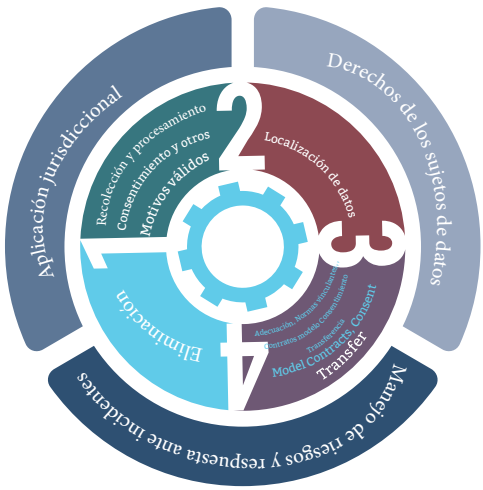
Enfoques regulatorios para la protección de datos

En el nivel nacional, la comunidad empresarial local debe prestar especial atención a los regímenes de protección de datos. Muchos países actualmente aprueban leyes y regulaciones en esta área; y hacer un balance de las normas relevantes ayudará a los grupos de defensa empresarial a trabajar con los responsables de elaborar políticas y otras partes interesadas a poner en práctica en enfoque más adecuado. Las empresas también pueden utilizar sistemas de protección de datos sólidos para impulsar la reputación de la marca, que desarrolla la confianza de los consumidores y usuarios. Si bien los regímenes de protección de datos suelen ser complejos, los temas clave que se tratan a continuación ayudarán a guiar a la comunidad empresarial local a medida que exploran esta área de la ley aún emergente.

Las diferentes jurisdicciones regulan la protección de datos de manera muy diferente con respecto al alcance y enfoque de las regulaciones. Algunas, como Japón, Ghana y la UE, han adoptado regulaciones integrales que cubren todas las actividades que involucran datos en un solo instrumento legal. Otras, como los EE. UU., regulan sector por sector.[52] Corea del Sur también es un ejemplo de lo último, con diferentes leyes que se aplican a la tecnología de la información (IT), transacciones financieras y la divulgación de información de crédito personal.[53] Si bien Brasil en la actualidad tiene un enfoque sectorial similar, tiene dos proyectos de ley bajo consideración que moverían al país hacia un marco amplio de protección de datos.[54] Las regulaciones también pueden diferir sobre la base de la sensibilidad de los datos (como en la UE y Rusia, donde requisitos más estrictos aplican a los datos sensibles; la capacidad y el impacto de datos de entidades (en Australia, las empresas con una facturación anual de $3 millones de dólares australianos o menos no están sujetos a la Ley de Privacidad);[55] o categorías especiales de personas (por ejemplo, los niños; la Ley de Derechos de los Niños N.º 26 de 2003 en Nigeria protege la privacidad de los niños menores de 18 años). Por último, algunas jurisdicciones con regímenes de protección de datos influyentes, como el Régimen de Protección General de Datos (GDPR), se centran más en el consumidor, y conceden un rango de derechos y poderes a los consumidores.[56]

En la práctica, los regímenes de protección de datos incluyen una combinación de instrumentos de política, como disposiciones, leyes, regulaciones y estándares constitucionales.[57] Sin importar los instrumentos legales, los elementos regulatorios comunes incluyen obligaciones que rigen los pasos en el ciclo de vida de los datos (recopilación y procesamiento, almacenamiento, transferencia y eliminación) y obligaciones transversales (respuestas a una violación de datos, la aplicación de leyes nacionales a empresas extranjeras, y los derechos de las personas a quienes se refieren los datos).[58] Estos elementos regulatorios se ilustran en el **Diagrama 2** y se explican en detalle a continuación.

Diagrama 2. Elementos regulatorios de los regímenes de protección de datos



Fuente: New Markets Lab (2018)

Enfoques regulatorios que aplican en diferentes etapas de estilo de vida de los datos

Recopilación y procesamiento: En muchas jurisdicciones, las compañías que pueden recopilar y procesar datos en el curso de sus operaciones comerciales deben tener justificativos válidos para hacerlo, incluso el consentimiento de los sujetos de los datos. A principios de 2018, Egipto estuvo cerca de finalizar un proyecto de ley que incorporaría un requisito de consentimiento y normas generales de protección de datos en la constitución egipcia.[59] Otros países también se están encaminado en esa dirección.

Almacenamiento: Muchas jurisdicciones requieren que los negocios almacenen datos en servidores físicamente ubicado dentro de sus fronteras nacionales. Estas normas se llaman requisitos de localización de datos. Algunos ejemplos incluyen Alemana, Kirguistán, Nigeria, Indonesia, Rusia, Grecia, China, Malasia y Australia.[60] Muchas empresas, particularmente las que operan en más de un país, informan que esos requisitos de localización de datos son una carga financiera y pueden desviar recursos financieros ya limitados. Para las empresas locales, estos requisitos pueden desalentar operaciones comerciales que dependen de los flujos de datos internacionales. En 2013, por ejemplo, se estimó que la construcción de centros de datos en Brasil y Chile costaría $60.3 millones de dólares estadounidenses y $43 millones de dólares estadounidenses, respectivamente.[61] Como se explica a continuación, algunos acuerdos de comercio internacional ahora incluyen disposiciones para frenar los requisitos de localización de datos, y la comunidad empresarial puede enfocar los esfuerzos de defensa para apoyar esta tendencia.

Transferencia de datos: Las jurisdicciones restringen la transferencia transfronteriza de datos a diferentes grados. A veces, se permiten transferencias bajo excepciones de única vez o continuas. Las excepciones de única vez (por ejemplo, para el cumplimiento de contratos) son comunes.[62] Sin embargo, las excepciones continuas se consideran de manera diferente según el caso, y generalmente requieren una evaluación de su hay un grado suficiente de protección de datos. Las transferencias continuas de datos suelen ser manejadas por jurisdicciones que

1. Evaluación de si las leyes nacionales de la jurisdicción que exporta los datos son adecuadas: en enfoque de adecuación, que pone la carga en el sector público;
2. Evaluación de si los mecanismos de revisión independientes de una empresa determinada son suficientes, como los sistemas de las Normas Corporativas Vinculantes (BCR) de la UE y Japón y las Normas de Privacidad Transfronteriza de la APEC (APEC CBPR): el enfoque de normas corporativas vinculantes, que pone la carga en el sector privado;
3. Evaluación sobre la base de las protecciones contractuales: el enfoque de contratos modelo, rara vez utilizado; o
4. Evaluación del consentimiento individual para la transferencia de datos: el enfoque del consentimiento, que pone la carga en el sector privado para demostrar consentimiento.[63]

reciben los datos en virtud de uno de los siguientes cuatro enfoques, con diferentes implicaciones para la comunidad empresarial local y los gobiernos que exportan los datos:

Entre estos, los primeros dos enfoques son los que más se siguen, aunque su aplicación puede diferir según la jurisdicción. Las partes interesadas con base en una jurisdicción con leyes de protección de datos débiles pueden preferir el enfoque de normas vinculantes corporativas. El enfoque de contratos modelo también podría ser una opción, pero se utiliza con mucha menos frecuencia (a la fecha, solo en la UE) y depende de la plena implementación de contratos modelo.[64] Por el otro lado, las partes interesadas ubicadas en una jurisdicción con normas de protección de datos sólidas pueden solicitar que su gobierno busque el "estado de adecuación" de otra jurisdicción, lo que racionalizaría la transferencia de datos en general. Las fortalezas y debilidades de cada enfoque se incluyen en la **Tabla 3**.

Eliminación: Una vez que los datos han cumplido con sus fines previstos (por ejemplo, cuando se completa una transacción), algunas jurisdicciones requieren la destrucción o eliminación de los datos. En dichas jurisdicciones, la comunidad empresarial local necesitaría monitorear con cuidado un amplio rango de hardware y software que se utiliza para el almacenamiento de datos para garantizar la completa eliminación de todos los datos relevantes. Las empresas también pueden necesitar designar o contratar administradores de retención de registros para garantizar la eliminación completa y segura, especialmente para los datos que se guardan en servicio en la nube.[65] Los grupos de defensa empresarial deben considerar las diferentes cargas impuestas en la comunidad empresarial local en virtud de diferentes leyes de eliminación, y apoyar los enfoques que se ajusten mejor a las necesidades de las PyMEs y las empresas más grandes.

Tabla 3. Enfoques para manejar las transferencias transfronterizas de datos

Enfoque	Fortalezas	Limitaciones
Adecuación	• Permite la transferencia completa (para las jurisdicciones que se determina que son adecuadas) • Promueve la interoperabilidad y armonización • "Lista blanca" transparente y abierta	• Causa dificultad considerable para las jurisdicciones que se determina que no son adecuadas • Dificultad para ajustarse a las jurisdicciones con diferentes enfoques con respecto a la protección de datos • Proceso largo para determinar la adecuación

Normas corporativas vinculantes	• Permite el movimiento libre de los datos dentro de un grupo corporativo • Promueve las buenas prácticas con respecto a los procesos de protección de datos y supervisión en el sector privado • Lista transparente y abierta de los países participantes	• Proceso de aprobación largo y costoso • Uso limitado para otras transferencia de datos fuera del grupo corporativo
Contratos modelo	• Promueve la interoperabilidad y armonización • Se pueden implementar rápidamente por parte de empresas individuales dispuestas a adoptar cláusulas textuales de contratos modelo	• Dificultad para desarrollar cláusulas modelo apropiadas y mantenerlas actualizadas • No hay transparencia con respecto a quién utiliza las cláusulas modelo • Oportunidad limitada para supervisión
	• Solución rápida y fácil para ciertos tipos de transacciones • No se requiere análisis o revisión detallada • Baja carga de cumplimiento para las empresas	• No es adecuado para muchas transacciones contemporáneas • Abierto para interpretaciones diferentes del consentimiento, y con tendencia a quejas y reclamos • Posibilidad de falta de imparcialidad en situaciones donde hay un desequilibrio de poder significativo entre las partes • Posibilidad de promover la fragmentación en lugar de la armonización de las prácticas de protección de datos

Fuente: Data Protection Regulations and International Data Flows: Implications for Trade and Development. 14. United Nations Conference on Trade and Development. Web. 2016 (modificado por New Markets Lab, 2018).

Enfoques regulatorios generales

Si bien las consideraciones regulatorias de arriba son específicas a las diferentes etapas del ciclo de vida de los datos, los temas a continuación aplican para todo el ciclo de vida y pueden tener un alcance más amplio.

Registro y notificación: Muchas empresas involucradas a lo largo del ciclo de vida de los datos deben registrarse ante el organismo regulatorio nacional o presentar notificación de las actividades. Si bien hay una variación en estos requisitos, pueden ser particularmente difíciles para las PyMEs y las nuevas empresas. Un tipo de requisito involucra notificar a las autoridades locales de protección de datos sobre los negocios o grupos de datos relevantes.[66] En Ghana, los controladores y procesadores de datos deben notificar a la Comisión de Protección de Datos desde el tipo de datos que la empresa mantiene hasta la naturaleza del procesamiento que la empresa realiza.[67] Como en otros países, las tarifas pueden ser considerables: en Ghana, a menudo ascienden a 750 cedis ghaneses o $167 dólares estadounidenses.

Para aligerar las cargas de cumplimiento de las empresas locales, los legisladores podrían redactar regulaciones con diferentes niveles sobre la base de los ingresos de la empresa o incluir otras exenciones incorporadas, similar a las exenciones en virtud de la Ley de Privacidad de Australia basada en los ingresos de la empresa.[68] Los compromisos regulatorios también se podría aplicar de manera incremental en función de la capacidad. Esto podría incluir períodos de gracia más largos para implementar ciertas obligaciones para las empresas de menos de un tamaño determinado.

En algunos casos, los esquemas de certificación de terceros están tomando el lugar del registro gubernamental formal. Estos incluyen el enfoque de normas corporativas vinculantes (BCR europeo y APEC CBPR). Este enfoque conlleva costos como los pagos de solicitud para el operador del esquema y servicios de certificación de terceros para la certificación anual. La desventaja de este enfoque es el tiempo que lleva (un promedio de 18 meses para obtener la certificación de la UE); de lo contrario, es mucho más sencillo.

Respuestas a la violación de datos: Para desarrollar un sistema que pueda soportar y minimizar el impacto de la violación de datos, muchas jurisdicciones han impuesto obligaciones con respecto al manejo de riesgos y la respuesta ante incidentes. Las regulaciones tienden a cubrir las medidas organizacionales, monitoreo y respuesta ante incidentes. En el nivel organizacional, algunos países, como la UE, Chuna, México y Filipinas, requieren el establecimiento y nombramiento de oficiales dedicados de protección de datos (DPO, por sus siglas en inglés). Es posible que se apliquen requisitos más estrictos para algunas organizaciones (como aquellas cuyo negocio principal gira en torno al procesamiento a gran escala de datos personales sensibles), y es posible que se requiera que los DPO cuenten con "conocimiento experto" de las leyes de protección de datos.[69] Los profesionales de protección de datos con experiencia escasean, y algunas empresas pueden necesitar tercerizar el rol del DPO a un proveedor externo, con un gran costo.[70]

Monitoreo: El monitoreo eficaz es esencial para detectar potenciales violaciones de datos más temprano. Algunas jurisdicciones

han adoptado un enfoque basado en riesgos, adoptando medidas de mitigación de riesgos adaptados al nivel de exposición. México, por ejemplo, requiere que las compañías lleven a cabo un análisis de riesgo de seguridad.[71]

Respuesta ante incidentes: Esto abarca las acciones que los gobiernos o las empresas deberán tomar en caso de una violación de datos. Algunas jurisdicciones tienen notificación obligatoria, incluso México[72] y los EE. UU.[73] Los requisitos varían en cuanto a su especificidad y cobertura, pero en general incluyen los siguientes elementos: 1) **quiénes deben cumplir con la ley, como empresas o entidades públicas**; 2) **cobertura de la información**; 3) **definición de una violación de datos**; 4) **requisitos de la notificación**, como cuándo se debe notificar y el método de notificación; y 5) **exenciones**, como la información encriptada.[74]

Derechos de los sujetos de los datos: Los sujetos de los datos son las personas que poseen los datos personales en uso. A veces, los gobiernos intervienen para proporcionar un rango de derechos para los sujetos de los datos, como los consumidores, que generalmente no tienen un poder de negociación suficiente para definir políticas de la compañía. Como se indica arriba, algunos de los regímenes de protección de datos más influyentes, especialmente la GDPR de la UE[75] (consulte el **Diagrama 3**) tienen un enfoque centrado en el consumidor con respecto a la protección de datos y conceden derechos de gran alcance a los consumidores. La GDPR también ha sido un modelo para las jurisdicciones que buscan centralizar sus mecanismos de aplicación y marcos de protección de datos, ambos se analizan con más detalle a continuación.

Diagrama 3: Derechos de los sujetos de los datos en la GDRP de la UE

Derecho a ser informado	Derecho de acceso	Derecho a rectificación	Derecho a eliminación ("Derecho a ser olvidado")
Derecho a ser informado sobre la recopilación y uso de los datos personales de los sujetos de los datos	Derecho a acceder a los datos personales e información complementaria de los sujetos de los datos	Derecho a corregir o completar datos personales inexactos o incompletos sin demora excesiva	Derecho de los sujetos de los datos a eliminar sus datos personales
Derecho a solicitar la restricción y supresión de los datos personales de los sujetos de los datos	Derecho a obtener y reutilizar los datos personales para los propios fines de los sujetos de los datos en diferentes servicios	Derecho a oponerse al marketing directo o procesamiento en limitadas circunstancias	Derecho a no estar sujeto a toma de decisiones automatizadas, incluso evaluación por perfil
Derecho a la restricción de procesamiento	**Derecho a la portabilidad de datos**	**Derecho a oponerse**	**Toma de decisiones automatizada**

Fuente: New Markets Lab (2018).

Algunos derechos pueden estimular la competencia en el mercado, incluso entre las PyMEs. Por ejemplo, un proyecto de ley en Brasil[76] permite que las partes interesadas de los datos soliciten portabilidad de datos: es decir, que una copia de sus datos se transmita directamente de un controlador a otro. La transmisión sin problemas de datos, posibilitada por la interoperabilidad entre diferentes sitios web y plataformas, podría promover el ingreso de nuevos participantes en el mercado y aumentar la competencia al servicio de los clientes potenciales que, de otro modo, no están dispuestos a volver a ingresar todos sus datos.[77]

Alcance jurisdiccional: Hay una creciente tendencia entre los organismos reguladores a aplicar leyes nacionales a todas las empresas de comercio electrónico extranjeras que se involucran con residentes nacionales, una práctica que se denomina alcance extraterritorial. Esto podría aumentar aún más los costos de cumplimiento para las empresas.[78] En Japón, la ley de protección de datos aplica expresamente a entidades extranjeras que recopilan y han recopilado información personal de cualquier persona que reside en Japón.[79]

La comunidad empresarial local debe considerar un rango de leyes, regulaciones y otras medidas que rigen la protección de datos, dependiendo de dónde residen los sujetos de los datos involucrados y las etapas relevantes en el ciclo de vida de los datos con los que están involucrados. Además, los grupos de defensa empresarial pueden presionar para un enfoque unificado con respecto a la transferencias transfronterizas de datos y una mayor armonización internacional.

Implementación y aplicación de la protección de datos

Hacer cumplir la protección de datos es un desafío continuo. Se destacan dos aspectos particular de aplicación, sanciones estrictas y el derecho de los agentes privados a reclamar compensación. Para los organismos reguladores que contemplan sanciones estrictas, y para la comunidad empresarial local bajo dicho régimen, es importante reconocer los posibles obstáculos. Por ejemplo, la violación de una ley de protección de datos en la UE puede resultar en multas basadas en los ingresos de hasta el cuatro por ciento de la facturación global anual, o sanciones penales en países como Japón, Filipinas y México.[80] Si bien las sanciones estrictas pueden alentar a las compañías a cumplir con las leyes de protección de datos, también pueden resultar en "forum shopping",”[81] y así afecta el efecto disuasivo de las multas estrictas. Estas medidas también afectan desproporcionalmente a las PyMEs, que no tienen la misma capacidad que las compañías multinacionales de ajustarse a los términos de servicio en respuesta a un cambio en la ley. En otros casos, los oficiales de aplicación (como los de China) pueden percibir que las multas son demasiado severas y aplicar alternativas menos estrictas, como advertencias administrativas.

Aparte de las sanciones, algunas jurisdicciones permiten que los consumidores presenten reclamos privados. Un ejemplo es la Ley de Protección de Datos de Ghana. La Ley establece un organismo estatutario independiente para investigar quejas, y establece expresamente el "Derecho Buscar Compensación a través de los Tribunales" como parte de los derechos de los sujetos de los datos.[82]

El cumplimiento de los regímenes de protección de datos puede ser costoso y complicado para

la comunidad empresarial local en general. Un informe la OECD resaltó que las compañías multinacionales gastaban más de $1 millón de dólares estadounidenses en costos de cumplimiento relacionados con los datos.[83] Para todas las demás empresas, mantenerse al día con una combinación de regulaciones globales y nacionales en evolución, sin hablar de cumplir con estas regulaciones, puede ser especialmente complicado. Se han identificado tres requisitos, que siempre están presentes en los marcos regulatorios nacionales, como particularmente complicados para las pequeñas empresas: 1) **requisitos de nombrar a oficiales de protección de datos**; 2) **requisitos de localización de datos**; y 3) **requisitos de registro**.

Para los gobiernos, hacer cumplir las leyes de protección de datos pueden ser un desafío debido a las limitaciones de capacidad y falta de concientización. Las campañas de concientización podrían ayudar a crear incentivos para que las empresas cumplan, y sin duda serían menos costosas que las acciones de aplicación de ley.[84] La Comisión sobre los Derechos Humanos y Justicia Administrativa en Ghana ha resaltado el desafío de aplicación y la necesidad de desarrollar capacidad legal y judicial.[85] A pesar de que la Comisión ha recibido algunas quejas sobre violaciones de datos, las acciones de cumplimiento de la Ley no se han aplicado activamente. Esas acciones requieren más concientización y capacidad entre las partes interesadas, incluso abogados fiscales y jueces para hacer aplicar eficazmente las sanciones aplicables.

Marcos institucionales relacionados con la protección de datos

Los marcos institucionales que rigen la privacidad de los datos tendrán una función central en cómo se rige el sector y cómo la comunidad empresarial local puede involucrarse con los responsables de elaborar políticas y otras partes interesadas. Cuando los marcos institucionales para la protección de datos varían de una jurisdicción a otra, los canales públicos o privados pueden estar disponibles para la defensa y aporte regulatorio. Algunos países permiten que los ciudadanos y miembros de la comunidad empresarial comenten sobre las leyes propuestas, incluso las que apuntan a regular la protección de datos. Brindar comentarios activamente para el proceso de elaboración de normas permite que las partes interesadas definan marcos que respondan a sus necesidades. Panamá es un ejemplo de participación en el proceso legislativo, como se mencionó en la Guía Resumida.

En el nivel nacional, muchos países trabajan para establecer un solo organismo regulador central para la protección de datos, con amplias responsabilidades legislativas y de supervisión.[86] Este enfoque facilita las obligaciones de cumplimiento para las compañías, proporciona un solo punto de contacto para los consumidores que buscan información o reparación, y establece estándares para minimizar la fragmentación regulatoria, tanto localmente y en el extranjero.[87] Estos organismos reguladores centrales han establecido pautas claras, han realizado desarrollo de capacidad con las empresas y han proporcionado un solo punto de contacto para las quejas de partes interesadas. Otras jurisdicciones dividen los roles regulatorios por sectores o funciones. Corea del Sur, por ejemplo, divide las funciones regulatorias y de administración de quejas entre dos agencias.[88]

Estudio de caso: Comentarios públicos sobre la Ley de Protección de Datos de Panamá

Las asociaciones empresariales puede participar activamente en el proceso de legislación para las leyes de protección de datos. Si bien el proceso en sí mismo varía considerablemente en las jurisdicciones, los procesos administrativos a veces permiten la participación y comentarios de la sociedad civil y los agentes privados. Un ejemplo es el desarrollo de una legislación de protección de datos en Panamá.

A mediados de 2016, el Congreso de Panamá presentó un proyecto para regular la protección de datos en el país. Celebró una audiencia pública de tres meses para recibir comentarios de agentes de la sociedad civil, ciudadanos privados y empresas. La audiencia pública fue realizada por la Autoridad Nacional para la Innovación Gubernamental y la Autoridad Nacional de Transparencia y Acceso a la Información, y tuvo la participación especial de la Organización de los Estados Americanos y el Tribunal Interamericano de Derechos Humanos, lo que significa que se consideraron marcos regionales e internacionales. Los participantes brindaron comentarios, que se incluyeron en el proyecto final presentado al Congreso de Panamá a principios de febrero de 2017. Para promover el debate público sobre el tema, diferentes organizaciones realizaron conferencias con un representante grande del sector privado (Google) y la Cámara de Comercio de Panamá.

Hasta septiembre de 2018, el proyecto no ha sido adoptado como ley debido a limitaciones de presupuesto. No obstante, el proceso de elaboración de normas en Panamá hace hincapié en la buena práctica de alentar a las asociaciones empresariales interesadas a formar parte en el proceso de elaboración de normas y expresar sus inquietudes. También se involucraron instituciones regionales e internacionales. De la misma manera, el Proyecto de Ley de Protección de Datos estuvo abierto a comentarios públicos hasta el 10 de septiembre de 2018.

Fuentes: IPANDETEC, Cronología de un Proyecto de Ley de Protección de Datos en Panamá, 29 de enero de 2018. Web; AIG, Consulta pública sobre Proyecto de Ley de Protección de Datos de Carácter Personal" refuerza el marco legal para la Economía y el Gobierno Digital, 11 de julio de 2016. Web; Violeta Villar, Panamá necesita aprobar Ley de Protección de Datos, El Capital, 14 de febrero de 2018. Web; Gobierno de Panamá, Avalan proyecto que establece la protección de datos de carácter personal, Consejo de Gabinete, 18 de enero de 2017. Web.

Análisis Profundo Legal – Ciberseguridad

La regulación sobre la ciberseguridad, que protege la tecnología de la información y los sistemas informáticos contra ataques, es un tema principal de preocupación para la comunidad empresarial global, entre otras partes interesadas. Los ataques recientes en computadoras y redes informáticas, tanto públicas como privadas, han crecido en escala y gravedad, perjudicando a gobiernos, la industria y a los consumidores. La ciberseguridad incluye ampliamente los activos de los agentes públicos y privados y cubre "dispositivos de computación conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida o almacenada".[89]

Este análisis profundo de los marcos legales y regulatorios que rigen la ley de ciberseguridad ilustrará las diferentes prácticas regulatorias que se utilizan en todo el mundo. También aborda las consideraciones clave para la comunidad empresarial y los organismos reguladores. Este análisis profundo comienza con una descripción general de los marcos regionales de ciberseguridad. Luego describe algunos enfoques regulatorios comunes con respecto a la ciberseguridad, los desafíos específicos relacionados con la implementación y aplicación de las leyes y regulaciones, y ejemplos de marcos institucionales relevantes. Además, la sección Ciberseguridad en la Guía Resumida contiene orientación empresarial y de defensa para la comunidad empresarial local, incluso una lista de verificación para analizar las leyes y regulaciones locales de ciberseguridad existentes.

Marco internacional para la ciberseguridad

Todos los países regulan la ciberseguridad de manera diferente, y aún no existe un conjunto vinculante de normas internacionales diseñadas para armonizar los sistemas nacionales. Los marcos internacionales, que incluyen convenciones, iniciativas y acuerdos comerciales, tienden a centrarse en torno a la cooperación internacional y desarrollo de capacidad. En general, no son ni detalladas ni prescriptivas. No obstante, como se centran en el desarrollo de capacidad y cooperación, son herramientas útiles y pueden ayudar a guiar los debates de política. La **Tabla 4** resume los marcos internacionales clave en relación con la ciberseguridad.

Tabla 4. Marco internacional y regional para la ciberseguridad

Marco	Implicaciones clave para la comunidad empresarial
Multilateral	
• Convención de Budapest • Acuerdo General sobre Comercio y Servicio (Acuerdo GATS, por sus siglas en inglés) de la Organización Mundial de Comercio (WTO) • Memorando de la Unión Internacional de Telecomunicaciones/ Oficina de las Naciones Unidas contra la Droga y el Delito[90]	• La Convención de Budapest impulsa la cooperación internacional y la elaboración de política global para combatir los delitos informáticos. Armoniza leyes penales nacionales con respecto a los delitos informáticos y proporciona pautas para promulgar procedimientos penales nacionales. No solo ayuda a establecer un estándar internacional, sino también proporciona orientación para debates nacionales entre la comunidad empresarial y los responsables de elaborar políticas con respecto a nuevas leyes, regulaciones y políticas. • El GATS requiere un trata no discriminatorio y transparencia una vez que un país se ha comprometido a abrir sectores nacionales para el comercio internacional. Las comunidades empresariales dentro de los estados miembro de WTO pueden utilizar esto como fundamento para mayor transparencia en la elaboración de normas y aplicación. • El Memorando de UN ITU ofrece asistencia técnica y capacitación legal para los oficiales de aplicación de la ley y otras partes interesadas. La organización también busca la experiencia de los miembros de la industria, creando un canal para el compromiso.

Regional	
• Organización para la Seguridad y Cooperación en Europa (OSCE)[91] • Código Internacional de Conducta para la Seguridad de la Información • Organización de los Estados Americanos (OAS) – Estrategia Integral Interamericana de Ciberseguridad.[92] • Las Pautas de OECD para la Seguridad de las Redes y Sistemas Informáticos[93] • CPTPP	• Los marcos regionales para la ciberseguridad contienen posiciones regulatorias de ejemplo que podrían informar las posiciones que la comunidad empresaria tomó a nivel nacional y con respecto a futuros acuerdos. • La OSCE crea medidas de desarrollo de confianza y alienta a los estados miembro a aumentar la cooperación pública-privada (sin embargo, esta disposición es voluntaria). • El Código Internacional de Conducta para la Seguridad de la Información establece que los estados deben "cooperar plenamente" con las partes interesadas, incluso el sector privado y la sociedad civil para mejorar la cultura en torno a la seguridad de la información. Este llamado a la cooperación con el sector privado puede proporcionar un canal para la participación. • La Estrategia de OAS desarrolla una red de advertencia regional para alertar e informar sobre incidentes entre los Miembros de OAS y comparte infraestructura segura para manejar las comunicaciones del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) con el sector privado y otras partes interesadas. • Las Pautas de OECD para la Seguridad de las Redes y Sistemas Informáticos son el resultado de una iniciativa de múltiples partes interesadas para modernizar un conjunto más antiguo de pautas de OECD. Este enfoque colaborativo dio como resultado pautas integrales para estrategias nacionales de ciberseguridad. • EL CPTPP contiene disposiciones que promueven la colaboración entre signatarios para asistir a las PyMEs para superar los obstáculos al comercio electrónico. Si bien no son vinculantes, podría ser un canal de defensa importante en los países de CPTPP.

Fuente: New Markets Lab (2018).

Enfoques regulatorios para la ciberseguridad

A pesar de estos esfuerzos internacionales y regionales, hay una variación considerable en cómo las jurisdicciones regulan la ciberseguridad. Los enfoques regulatorios han evolucionado en tres oleadas con el correr del tiempo. La primera oleadas de regulación se enfocó en la legislación sobre delitos informáticos, un enfoque descendiente que comienza con organismos reguladores y acción del gobierno. La segunda fase involucró la aplicación de normas y estándares de leyes cibernéticas de múltiples partes interesadas dirigidas por el sector privado. Esta oleadas comenzó después de la crisis financiera mundial de 2008. La tercera fase consiste en una legislación de ciberseguridad más integral, que se ha vuelto común en los últimos años. El **Diagrama 3** muestra las tres fases de las regulaciones de ciberseguridad, que se tratarán con más detalle a continuación.

Diagrama 3. Evolución de las regulaciones de ciberseguridad

Legislación sobre delitos informáticos

Primer tipo de regulación de ciberseguridad adoptada en la mayoría a través de un enfoque descendiente. Los delitos informáticos más comunes incluyen:

- Suplantación de correo electrónico
- Fraude electrónico
- Correo no solicitado
- Difamación cibernética
- Acoso cibernético
- Robo de identidad
- Piratería de software
- Acceso no autorizado
- Negación de servicio
- Anulación de web
- Ransomware (cibersecuestro de datos)
- Ataque Salami
- Bomba lógica
- Estafa de datos

Aplicación de múltiples partes interesadas dirigidas por el sector privado

El desarrollo privado de un programa, procedimientos y estándares de ciberseguridad se institucionaliza a través de un marco de múltiples partes interesadas

Regulación integral de ciberseguridad

Las regulaciones generales recientemente promulgadas abordan:

- Cobertura (general o específica del sector)
- El aspecto preventivo (mecanismos estratégicos, organizacionales y de monitoreo), y
- El aspecto reactivo (definición de incidente cibernético o ataque cibernético y las obligaciones legales impulsadas por el incidente cibernético o el ataque cibernético)

Fuente: New Markets Lab (2018)

Las jurisdicciones tienden a caer en una de estas tres fases. A medida que el marco legal y regulatorio continúa cambiando, la comunidad empresarial puede tener diferentes necesidades de defensa, según el lugar en el ciclo en que se encuentre su jurisdicción. Los matices particulares de cada una de estas fases se describen a continuación.

Legislación sobre delitos informáticos

Diagrama 4. Tipo comunes de delitos informáticos

Tipos de delitos informáticos	Fraude electrónico	Correo no solicitado	Difamación cibernética	Acoso cibernético
	El acto de intentar adquirir de manera fraudulenta información personal confidencial como, por ejemplo, contraseñas y datos de tarjetas de crédito, asumiendo la identidad de otra persona en un correo electrónico de aspecto oficial, mensaje instantáneo, etc.	Publicidades comerciales no deseadas que se envían por correo electrónico en internet. Hay una ley que aborda el correo no solicitado en, al menos, 33 países, incluso la UE.	Declaración de hecho falsa y sin privilegios que es dañina para la reputación de alguien y que se publica "con falta", es decir, como resultado de negligencia o malicia.	Usar internet, el correo electrónico u otros tipos de comunicaciones electrónicas para acosar, hostigar o amenazas a otra persona.
Acceso no autorizado/ hackeo	**Negación de servicio**	**Deformación de sitio web**	**Ransomware (cibersecuestro de datos)**	**Ataque Salami**
Acercarse, ingresar sin autorización, comunicarse, almacenar datos, recuperar datos o interceptar y cambiar los recursos informáticos sin consentimiento, incluidos hackeo, malware y ataques de virus.	Cuando un atacante inunda el ancho de banda o los recursos de un determinado sistema o servidores con tráfico, lo que impide que los usuarios legítimos accedan a información o servicios.	Tomar control de un sitio web de manera fraudulenta ya sea para cambiar el contenido del sitio original o para redirigir al usuario a otra página falsa de apariencia similar, controlada de forma fraudulenta por otra.	Forma de software maliciosos que se infiltra en las redes o sistemas informático y usa herramientas como encriptado para negar el acceso o mantener los datos como "rehén" hasta que la víctima pague un rescate, y con frecuencia exige pagos en Bitcoin.	El delito cibernético generalmente utilizado para el propósito de cometer delitos financieros donde los delincuentes roban dinero o recursos poco a poco de cuentas financieras en un sistema.
Piratería de software	**Robo de identidad**	**Bomba lógica**	**Estafa de datos**	**Suplantación de correo electrónico**
El copiado/ distribución no autorizada de software.	Obtener o usar de manera indebida los datos personales de otra persona de alguna manera que involucre fraude o engaño, generalmente para beneficio económico.	Código de programación oculto en un programa o sistema que causa que suceda algo cuando el usuario realiza una determinada acción o cuando se cumplen ciertas condiciones.	Cambio no autorizado de datos antes o después de su ingreso en un sistema informático. Algunos ejemplos son falsificar o adulterar documentos e intercambiar cintas o tarjetas informáticas válidas con reemplazos preparados.	Manipular el correo electrónico comercial para falsificar el verdadero origen del correo electrónico, sin el consentimiento o autorización del usuario cuyo correo electrónico dirigido está falsificado.

Fuente: New Markets Lab (2018).

La legislación inicial sobre ciberseguridad se enfocó principalmente en la prevención de un rango de delitos informáticos. El **Diagrama 4** de arriba contiene ejemplos de los tipos más comunes de delitos informáticos. Las jurisdicciones regulan los delitos informáticos hasta la fecha, y siguen siendo una parte importante de la seguridad general en línea.

La legislación sobre delitos informáticos nunca será completamente efectiva sin sanciones suficientes y capacidad de aplicación. Por ejemplo, en 2012, Brasil aprobó su primera ley de delitos informáticos, que estaba acompañada de sanciones leves como arresto domiciliario, y aplicada por divisiones de delitos informáticos con poco personal y financiación.[94] A pesar de la promulgación de esta ley, en 2017 Brasil aún estaba clasificada como el país con más víctimas de delitos informáticos en Latinoamérica; los delitos principales eran malware y fraude en línea.[95]

Aplicación de múltiples partes interesadas dirigidas por el sector privado

Además de la legislación sobre delitos informáticos, la aplicación liderada por el sector privado ayuda a guiar las empresas que buscan establecer sistemas preventivos contra posibles riesgos de ciberseguridad. Este enfoque armoniza las buenas prácticas de la industria (programas, pautas y estándares) y las adapta en un marco compuesto por socios de gobierno, la industria, académicos e internacionales.[96] Para las empresas, alinearse con estas prácticas podría ayudar a priorizar la inversión en la ciberseguridad. Muchas de estas pautas permiten la adopción flexible, personalizada según el tamaño y naturaleza de la empresa.[97]

Es esencial que la comunidad empresarial local se mantenga al día con respecto a estas prácticas. Si bien estos marcos son voluntarios, no cumplir con las buenas prácticas ampliamente adoptadas podría poner a las empresas en desventaja competitiva. Quizás lo más importante es que esta es una manera para que las empresas se involucren temprano en el proceso de elaboración de leyes y participen en el diálogo público-privado con respecto a las buenas prácticas.

El RU ha incorporado la adopción voluntaria de pautas de seguridad a su Estrategia de Ciberseguridad del RU de 2011.[98] Una característica interesante de esta estrategia es el programa de certificación en Aspectos Esenciales Cibernéticos, que crea incentivos para la adopción de controles de seguridad básicos. Este programa es obligatorio para los contratistas del gobierno del RU que manejan información personal.[99] El gobierno del RU, a través de Hojas de Consejos sobre el los 10 Pasos para el Programa de Ciberseguridad, facilita el proceso por el cual las compañías de cualquier tamaño pueden obtener certificación en Aspectos Esenciales Cibernéticos. Estas medidas accesibles son particularmente beneficiosas para las PyMEs, que pueden utilizar la certificación como una manera para mejorar la confianza del consumidor en productos y servicios.[100]

Legislación integral de ciberseguridad

Para complementar los marcos de delitos informáticos y de múltiples partes interesadas, muchas jurisdicciones han definido nueva legislación integral de ciberseguridad. Bajo estos marcos, se requiere con frecuencia que las empresas tengan ciertos sistemas, tecnologías o planes para proteger la seguridad en línea. Aquellas involucradas en infraestructuras críticas, como redes eléctricas, pueden estar sujetas a requisitos adicionales para fines de seguridad nacional. Cabe destacar aquí que un enfoque excesivamente restrictivo, como los que se utilizan en Rusia, Chima y Vietnam, podría afectar negativamente el flujo de información, con implicaciones significativas para el comercio internacional y la libertad de expresión.[101]

Estos marcos integrales a menudo tienen requisitos más estrictos en relación con el informe posterior de incidentes cibernéticos. Esto difiere de las regulaciones que usan un enfoque orientado a los resultados. Este enfoque considera que un evento es un incidente cibernético cuando realmente se viola el sistema de información. Este enfoque está en vigencia en Rusia.[102] Otro método se enfoca en el intento de violación, que es suficiente para constituir un incidente cibernético en sí mismo. Los EE. UU.[103] y Singapur[104] se adhieren a este modelo. Cuando determinan qué enfoque defender, la comunidad empresarial local debe considerar si pueden cumplir adecuadamente y responder a un enfoque más expansivo. Si esto sería excesivamente complicado, el enfoque orientado a los resultados podría ser una mejor opción.

El informe y otros procedimientos de mitigación también son aspectos comunes de un enfoque regulatorio integral. Las disposiciones no siempre requieren notificaciones oportunas y detalladas. Por ejemplo, el gobierno federal de los EE. UU. no requiere el informe de incidentes,[105] mientras que Rusia requiere que los bancos informes al Banco Central sobre cualquier incidente cibernético que amenace la seguridad de los datos en las transacciones de pago.[106] La UE es aún más prescriptiva y granular en su enfoque. En la UE, la legislación ha evolucionado para requerir informe de incidentes solo a algunos sectores, como la industria de las telecomunicaciones y proveedores de servicios digitales.

Implementación y aplicación de la ciberseguridad

Así como un sistema sólido y resistente es esencial para los agentes públicos y privados, también puede representar un desafío. A los organismos reguladores les puede resultar difícil mantenerse al día con los cambios en la tecnología relevante y sus aplicaciones. Incluso cuando hay marcos legales y regulatorios de ciberseguridad, surgen dificultades con la implementación y aplicación. Las PyMEs a menudo son las víctimas principales de los ataques cibernéticos, se enfrentan a una variedad de desafíos para cumplir con las

regulaciones obligatorias y los estándares voluntarios de la industria. Un estudio del Ponemon Institute en 2017 demostró que los ataques cibernéticos que afectan las PyMEs habían aumentado de 55 a 61 por ciento en el transcurso de un año.[107] La mayoría de estos ataques eran fraude electrónico o ingeniería social. A pesar de la prevalencia de los ataques cibernéticos, varias cuestiones de política clave interfieren con la adopción de medidas de ciberseguridad de parte de las PyMEs. Estas deben servir como temas que generan controversia para que la comunidad comercial local se involucre con el público y los responsables de elaborar políticas.

La primera cuestión es la falta de inversión en ciberseguridad. Por ejemplo, la mayoría de las PyMEs en Singapur gastan mucho menos del uno por ciento de sus ingresos en ciberseguridad, cifra que el Foro Económico Mundial considera el promedio de la industria necesario para todas las industrias de tecnología de la información y las comunicaciones (ICT) para combatir el delito cibernético. Esta falta de inversión es tal vez el resultado de la idea errónea de las PyMEs que las amenazas cibernéticas solo afectan a las organizaciones grandes o a compañías de tecnología de la información y comunicaciones (ICT). Por ejemplo, un informe de Juniper Research demostró que el 74 por ciento de las PyMEs en el RU piensa que están a salvo de ataques cibernético, incluso cuando admiten que han sufrido violaciones a los datos.[108]

En el sector privado, la falta de espacio en el presupuesto para combatir la ciberseguridad es otra causa principal de la falta de inversión de las PyMEs.[109]Puede ser costoso para las PyMEs invertir en hardware, software y transformación organizacional necesarios para implementar las regulaciones y estándares relevantes. El monto de referencia que se requiere para una protección mínima[110] puede fácilmente exceder el presupuesto de una PyME, que a menudo está vinculado a los ingresos o el gasto ICT.[111] Además, las PyMEs en general carecen de personal interno. Esto no solo causa dificultad para proteger adecuadamente los sistemas informáticos, sino también una incapacidad de interpretar adecuadamente los estándares técnicos o actualizar software de manera oportuna.[112] Esta dificultad práctica se ve agravada por el hecho de que muchos estándares técnicos carecen de pautas de implementación, lo que dificulta que las PyMEs cumplan independientemente.[113] Las empresas más grandes y las PyMEs podrían desarrollar pautas de implementación comunes, lo que aliviaría la carga de las PyMEs.

En un nivel sistémico, una de las razones para la inaccesibilidad es el hecho de que los estándares han sido desarrollados para organizaciones más grandes, que tienden a tener presupuestos más grandes y equipos de defensa y ciberseguridad dedicados. Existe una sensación entre las PyMEs de que los estándares técnicos simplemente no abordan adecuadamente sus problemas y desafíos.[114] La **Tabla 5** a continuación enumera algunos marcos populares de ciberseguridad que pueden brindar un punto de referencia para la comunidad empresarial local ya que considera qué enfoque legal y regulatorio se ajusta mejor a las necesidades de la comunidad. Al decidir el marco de estándares apropiados, los grupos de defensa y las empresas deben considerar los siguientes factores: 1) **si el marco se aplica a la empresa o la industria**; 2) **si los estándares requeridos brindan protección adecuada**; 3) **el rol de la empresa, como compradora o proveedora**; y 4) **el contexto de uso.**[115]

Tabla 5. Estándares de ciberseguridad

Marco	Organismo para la elaboración de estándar	Componentes clave
ISO/IEC 27001	Organización Internacional de Normalización (ISO) y Comisión Internacional Electrotécnica (IEC)	• Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de manejo de seguridad de la información en una organización. • Los requisitos son genéricos y están destinados a ser aplicados por todas las organizaciones, independientemente de su tipo, tamaño o naturaleza, lo que los hace ampliamente utilizados y recomendados.
Matriz de Controles en la Nube	Alianza de Seguridad en la Nube	• Brinda un entendimiento detallado de los conceptos y principios de seguridad en 13 dominios-
NIST CSF	Instituto Nacional de Estándares y Tecnología	• Abarca funciones: Identificar, proteger, detectar, responder y recuperar. • Divide la implementación en niveles, bajo los cuales una compañía puede elegir qué tan estricto es el marco de ciberseguridad que desea implementar.[116]
Controles de seguridad críticos	SANS Institute	• Incluye una lista de 20 controles que están diseñados para prevenir los ataques cibernéticos y facilitar la recuperación. Los ejemplos incluyen la creación de inventario y control de activos de hardware y software, manejo continuo de vulnerabilidad y respuesta y manejo de incidentes.[117]

Fuente: New Markets Lab (2018).

Marcos institucionales relacionados con la ciberseguridad

Debido a la naturaleza de múltiples niveles y altamente técnica de la ciberseguridad, los gobiernos deben considerar un marco institucional holístico para respaldar el marco legal. Las diferentes funciones para considerar incluyen: 1) **organismos legales y regulatorios para implementar normas y regulaciones**; 2) **capacidad técnica para identificar y responder a amenazas cibernéticas**, como el ejemplo del Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática en Rwanda, el Equipo de Respuesta para Emergencias Informáticas de Mauricio (CERT-MU),[118] y CERT en el RU; 3) **desarrollo de capacidad para lograr concientización**, brindar capacitación y desarrollar recursos; y 4) **cooperación entre socios entre agencias, nacionales y subnacionales e internacionales**.[119]

Las herramientas de ciberseguridad fueron principalmente desarrolladas por empresas y luego fueron transformadas en regulaciones. Participar activamente en cualquier proceso regulatorio beneficiaría a los negocios permitiéndoles compartir inquietudes con los responsables de elaborar políticas. Las compañías también podrían ayudar a diseñar programas que aborden sus necesidades particulares de ciberseguridad a través de un diálogo con el sector público.

A veces, un marco institucional específico del sector puede proteger la ciberseguridad en sectores particularmente sensibles. En Sri Lanka, una colaboración entre el Banco Central de Sri Lanka y el Equipo de Respuesta para Emergencias Informáticas de Sri Lanka, dirigido y financiado completamente por el sector bancario, ha llevado a la creación de un Equipo de Respuesta ante Incidentes de Seguridad Informática del Sector Financiero (FINCSIRT, por sus siglas en inglés). FINCSIRT recibe, procesa y responde a alertas de seguridad informática e incidentes que afectan a bancos y otras instituciones financieras certificadas en el país.[120] El estudio de caso que se encuentra en la Guía Resumida en la página 30 describe cómo Túnez creó un grupo de trabajo para ayudar a fortalecer los marcos de ciberseguridad.

Análisis Profundo Legal – Pagos electrónicos (e-payments)

El comercio electrónico permite que los diferentes agentes de la cadena de suministro intercambien bienes y servicios a través de plataformas digitales. Una transacción electrónica o e-transaction ocurre cuando agentes celebran un acuerdo a través de redes informáticas de brindar bienes o servicios. Las transacciones electrónicas de bienes requieren que el comprador autorice y realice un pago a través de medios digitales y que el vendedor autorice el envío o suministro de un servicio. Cuando este es el caso, el sistema legal clasifica estas autorizaciones como firmas electrónicas y el pago se convierte en un pago electrónico.

Los pagos electrónicos han sido ampliamente adoptados en años recientes gracias a la penetración masiva de teléfonos móviles y teléfonos inteligentes en todo el mundo. De manera similar, las firmas electrónicas son fundamentales no solo para autorizar pagos electrónicos, sino también para realizar otros tipos de contratos electrónicos, que ahora surgen como reemplazo de los contratos manuales. Los enfoques regulatorios deben equilibrar diferentes consideraciones de política, incluso eficiencia, transparencia y seguridad.

Este análisis profundo de los marcos legales y regulatorios que rigen las transacciones electrónicas en línea presenta algunos ejemplos de los diferentes enfoques regulatorios con respecto a los pagos electrónicos y firmas electrónicas que se utilizan en todo el mundo. También aborda las consideraciones clave para la comunidad empresarial local y los organismos reguladores a medida que más países comienzan a promulgar e implementar marcos de pagos electrónicos y firmas electrónicas. Este análisis profundo comienza con una descripción general de los mercados internacionales y regionales que ya existen con respecto a los pagos electrónicos. Luego describe algunos enfoques regulatorios comunes, los desafíos específicos relacionados con la implementación y aplicación de las leyes y regulaciones, y ejemplos de marcos institucionales . La sección Transacciones electrónicas en la Guía Resumida contiene orientación empresarial y de defensa para la comunidad empresarial local, incluso una lista de verificación para analizar las leyes y regulaciones locales existentes sobre las transacciones electrónicas.

Marcos internacionales y regionales para los pagos electrónicos

A medida que los mercados nacionales se conectan cada vez más en el nivel internacional a través del comercio electrónico y el comercio digital transfronterizos, será más necesario un solo sistema internacional de pago electrónico o un conjunto de estándares para facilitar las transacciones viables, convenientes y asequibles. Los pagos electrónicos internacionales dependen de la habilidad de los diferentes sistemas de servicio de pago de trabajar en colaboración, lo que es difícil de alcanzar debido a una falta de regulaciones armonizadas y variaciones entre las diferentes plataformas.[121] La comunidad empresarial debe sostenerse con opciones de pago electrónico limitadas, que actualmente incluyen compañías de tarjetas de crédito y servicios globales como PayPal. Se necesitarán marcos legales y regulatorios más dinámicos si la ley requiere mantenerse al día con la innovación de manera que ayude a los mercados a crecer. Dicho esto, existen varios marcos multilaterales y regionales o se están negociando en relación con los pagos electrónicos, que brindan ejemplos útiles de cómo abordar la regulación de los pagos electrónicos. Estos marcos se resumen en la **Tabla 6**. En particular, los marcos regionales brindan ejemplos más específicos de enfoques regulatorios, que pueden informar la participación de la comunidad empresarial a nivel nacional y en el contexto de futuros acuerdos.

Tabla 4. Marco internacional y regional para la ciberseguridad

Marco	Implicaciones clave para la comunidad empresarial
Multilateral	
• Acuerdo de Comercio de Servicios de la OMC (en negociación) • Iniciativa global de inclusión financiera del Banco Mundial (no vinculante)	• El Acuerdo de Comercio de Servicios de la OMC tiene como objetivo aumentar la liberación de servicios y expandir el acceso al mercado de servicios, incluyendo servicios financieros. Por lo tanto, los sistemas de pago electrónico (y los proveedores de pago electrónico como proveedores de servicios) se verán afectados. Este acuerdo, que se encuentra aún en negociaciones podría ser una prioridad para las iniciativas de defensa internacional. • La Iniciativa global de inclusión financiera del Banco Mundial reúne tanto a gobiernos como al sector privado para mejorar el acceso a la financiación y mejorar la confianza de los consumidores en diferentes formas de pago electrónico en los tres países piloto (México, Egipto y China). 84 Parte II – Análisis Profundo Legal Regional

Regional	
• NAFTA (en negociaciones) • CPTPP • Directiva del Parlamento Europeo y Consejo sobre Servicios de pago en el Mercado interno (PSD2)	• Los marcos de pago electrónico a nivel regional contienen enfoques regulatorios de ejemplos, que podrían informar las posturas tomadas por la comunidad empresarial doméstica y respecto de acuerdos futuros. • Los pagos electrónicos son un tema clave en las renegociaciones del NAFTA. • El CPTPP obliga a las partes a evitar cualquier carga regulatoria innecesaria sobre las transacciones electrónicas y es progresiva en el hecho de que facilita las opiniones de las personas interesadas en el desarrollo de los marcos nacionales para transacciones electrónicas. Esto brinda a la comunidad empresarial dentro de cada país miembro del CPTPP un canal más directo para la participación en el proceso nacional de creación de políticas. • El PSD2 sirve como un ejemplo de un requerimiento más restringido a nivel regional, ya que las empresas deben tener autorización para operar. El PSD2 establece controles sobre los requerimientos de registro y estándares de seguridad de la organización empresarial.

Fuente: New Markets Lab (2018).

Enfoques regulatorios para los pagos electrónicos

Los sistemas de pago electrónicos están regulados por la misma razón que los servicios financieros tradicionales. Los gobiernos quieren promover la inclusión financiera, proteger a los consumidores (que en general no tendrán la misma cantidad de información que el proveedor de servicios de pago electrónico) y promover un entorno saludable para las empresas e inversiones. Las compañías, por supuesto, querrán cumplir con la creciente demanda del mercado a través de canales electrónicos de una manera flexible y dinámica.

La regulación de los pagos electrónicos tiende a clasificarse en dos categorías:

pagos electrónicos tradicionales o bancarios, y pagos electrónicos no bancarios. Estas categorías se regulan de manera diferente. Los pagos electrónicos bancarios son los que se conectan a sistemas bancarios e incluyen tarjetas de débito, tarjetas de crédito y cuentas de la Cámara de Compensación Automatizada (ACH). Los sistemas de pagos electrónicos no bancarios son los provistos por intermediarias no bancarias. Algunos ejemplos incluyen Bitcoin, M-Pesa y billeteras digitales como PayPal y Alipay.

En general, los pagos electrónicos bancarios están regulados estrictamente en todo el mundo, y la mayoría de las jurisdicciones incorporan disposiciones sobre prevención y cumplimiento, autenticación de las transacciones, investigación y aplicación. En contraste, los sistemas regulatorios para los pagos electrónicos no bancarios a menudo siguen uno de dos enfoques: un enfoque ex ante que impone los controles regulatorios en sistemas de pago electrónico no bancarios, y un enfoque ex post enfocado en la aplicación, con condiciones menos restrictivas para el ingreso en el mercado. El **Diagrama 4** resume los enfoques regulatorios actuales, y las siguientes secciones brindan más detalles sobre cada uno de los tipos de sistemas de pago electrónico.

Diagrama 4. Enfoques regulatorios sobre el pago electrónico

Fuente: New Markets Lab (2018)

Pagos electrónicos bancarios

Para muchos comerciantes y consumidores, el acceso al sistema bancario es el primer obstáculo en el comercio electrónico y tradicional. De acuerdo con el Banco Mundial, en 2014, 2 mil millones de adultos carecían de acceso al sistema bancario o tenían poco acceso; el 55 por ciento de estos adultos eran mujeres.[124] Algunos minoristas y sus potenciales clientes a menudo se enfrentan a altos costos bancarios; también pueden carecer de la documentación necesaria para abrir cuentas bancarias, o fondos para costos indirectos (como viajar hacia un banco o cajero automático). Otros obstáculos incluyen informalidad económica o laboral, analfabetismo financiero y necesidades no abordadas de género, religiosas o culturales; y analfabetismo financiero[125]. En general, los organismos reguladores apuntan a superar estos desafíos al imponer la carga en las empresas que adoptan pagos electrónicos bancarios para cumplir con los requisitos legales.

Los enfoques regulatorios en todo el mundo están comenzando a converger. En la mayoría de las jurisdicciones, los aspectos clave incluyen:

Prevención y cumplimiento: Los organismos reguladores en general trabajan para asegurar que se completen los pagos electrónicos de una manera justa y transparente. A medida que los grupos defensores exijan reformas o nuevas regulaciones sobre el pago electrónico, deben determinar el mejor curso de acción sobre la base de las necesidades de las organizaciones miembro. Los organismos reguladores deben tener en cuenta que todas las partes

- **Licencia:** Muchas jurisdicciones, como Australia[126] y Suiza,[127] requieren que los emisores de tarjetas, como los bancos o instituciones financieras, obtengan licencias para operar;

- **Debida diligencia:** Las empresas interesadas en brindar pagos electrónicos bancarios deben cumplir con las obligaciones de informe relacionadas con otros asuntos de política, como programas contra el lavado de dinero, contra el terrorismo y transparencia impositiva,[128] incluso estándares internacionales contra el lavado de dinero;[129] y

- **Protección del consumidor:** Para cumplir con las obligaciones de protección del consumidor, los organismos reguladores a menudo requieren que las empresas 1) **divulguen adecuadamente el costo, los términos y condiciones de la transacción antes de la autorización** (como en Paraguay,[130] México,[131] y la UE[132]); 2) **limitar los costos que cobran a los clientes**, incluso los costos de la tarjeta de crédito y débito;[133] y 3) **limitar la responsabilidad financiera de los consumidores por costos no autorizados**, **mercaderías que se ordenaron pero nunca se recibieron, bienes y servicios no aceptados por el cliente, cargos duplicados y otros cargos incorrectos en la transacción** (como en Colombia,[134] Argentina,[135] y Kenia,[136] por ejemplo).

interesadas en un pago electrónico tienen cierto equilibrio de derechos y obligaciones. Si bien estas obligaciones difieren según la jurisdicción, algunas de las medidas de prevención y cumplimiento más comunes son:

Autenticación de las transacciones en línea: Los comerciantes tienen la obligación de brindar un entorno seguro para las transacciones, y diferentes sistemas regulatorios aplican a una variedad de mecanismos de autenticación. El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) se ha convertido en un estándar global de la industria[137] que determina los requisitos de autenticación sobre la base del tamaño de la compañía.[138]

Investigación: Muchas jurisdicciones tienen protecciones estrictas para los clientes que informan transacciones sospechosas o no aprobadas.[139] En dichos sistemas, cuando un cliente cancela una transacción o informa una transacción sospechosa para evitar costos de devolución, las instituciones bancarias deben iniciar una investigación de la tarifa impugnada, y seguir los plazos de tiempo legales aplicables en las diferentes jurisdicciones.[140] Si un comerciante no aborda una queja del cliente en tiempo y forma, o si no usa la debida diligencia para confirmar la identidad del titular de la tarjeta, la red de tarjetas cobrará una tarifa de procesamiento y un costo de devolución.[141]

Aplicación: Notablemente, muchos sistemas de pago electrónico bancario utilizan la aplicación privada a través de la autorregulación de la industria. Por ejemplo, en virtud del PCI DSS, la falta de cumplimiento puede resultar en sanciones por parte de la red de tarjeta, como por ejemplo, multas y cancelación de cuentas del comerciante.[142] Los desafíos relacionados con la aplicación de los pagos se cubren con más detalle a continuación.

Pagos electrónicos no bancarios

A diferencia de los pagos electrónicos tradicionales bancarios o basados en cuentas, los pagos electrónicos no bancarios tienden a ser regulados de manera diferentes en diferentes países. En general, las regulaciones caen en un espectro, y la comunidad empresarial local debe determinar dónde en este espectro se encuentra su jurisdicción. Por un lado se encuentra la regulación ex ante, donde los organismos reguladores determinan de manera proactiva los requisitos para ingresar y operar en el mercado antes de lanzar el servicio. Por el otro lado se encuentra la regulación ex post, donde los reguladores optan por monitorear los sistemas de pagos existentes en lugar de elaborar normas adicionales sobre el ingreso y operación en el mercado. El estilo ex post tiende a promover el crecimiento dinámico en la industria, aunque los sistemas ex post al principio pueden representar desafíos de capacidad para algunos países. Además, es posible que los países con un enfoque regulatorio más ex ante se cambien a sistemas más estructurados con el correr del tiempo.

Regulación ex ante: Las empresas en jurisdicciones ex ante deben obtener la aprobación para operar a través de 1) **una aprobación regulatoria según el caso** (generalmente por las mismas instituciones que supervisan el sistema bancario) o 2) **una regulación más amplia**. India es un ejemplo del enfoque según el caso, donde el Banco de Reserva de la India debe aprobar previamente cualquier nuevo sistema de pago propuesto.[143] La UE tiene un enfoque ex ante amplio a través de la PSD2, que regula todos los pagos electrónicos, incluso los pagos electrónicos no bancarios, a través de nuevas categorías de instituciones y servicios relacionados con la iniciación de pago y la información de cuenta. Ambos enfoques pueden beneficiar a la comunidad empresarial local, pero también tienen algunas desventajas. La aprobación según el caso podría preservar la flexibilidad regulatoria para nuevas tecnologías, pero los largos procesos de solicitud y la necesidad de familiarizar a los organismos reguladores con los nuevos sistemas y tecnologías pueden ser un problema para las empresas más pequeñas. Si bien la regulación amplia puede parecer más fácil para promover la concientización y participación de las partes interesadas, este tipo de enfoque tiende a ser un poco menos flexible.

Regulación ex post: Con este enfoque, los servicios de pago electrónico son monitoreados de cerca pero no están necesariamente sujetos a las regulaciones de ingreso en el mercado. Las empresas tienden a favorecer un enfoque ex post por su facilidad de ingreso en el mercado. Dicho enfoque también puede ayudar a promover la innovación, porque las empresas no necesitan preocuparse de que su tecnología dejará de ser válida conforme a la ley.[144] El sistema de transferencia de dinero móvil de Kenia M-PESA es un buen ejemplo (consulte el estudio de caso a continuación).

Estudio de caso:
La regulación de M-Pesa en Kenia

M-Pesa es un sistema de pago móvil no bancario que solo requiere el uso de un teléfono móvil y SMS y ha contribuido a reducir la desigualdad financiera en Kenia. Si bien M-Pesa tiene licencia como institución no bancaria, las cuentas bancarias están reguladas por leyes bancarias estrictas. Esto mantiene M-Pesa financieramente estable. El Banco Central de Kenia monitorea de cerca las actividades de M-Pesa, pero no ha promulgado regulaciones adicionales.

Los procesos de instalación y registro de M-Pesa son sencillos y gratuitos. Aproximadamente 36,000 comerciantes aceptaron pagos a través de M-Pesa desde 2016. Los usuarios depositan crédito a través de depósitos de efectivo o una aplicación que le permite al usuario vincular su cuenta bancaria a su cuenta de M-Pesa. Una vez que el dinero está en el sistema de M-Pesa, el usuario puede transferir fondos a amigos, familiares o comerciantes a través de un mensaje de texto. El precio de cada transacción depende de la estructura escalonada, lo que permite que hasta los clientes más pobres puedan acceder a la red. Cuando M-Pesa recibe el efectivo o los fondos, se depositan en cuentas bancarias y se mantienen en fideicomiso.

Si bien algunos modelos similares tuvieron éxito en varios países, incluso Paraguay, Honduras y El Salvador, los modelos bancarios móviles han tenido menos éxito en lugares como Sudáfrica y la India. En teoría, el modelo tiene amplia aplicabilidad, y necesita solo un proveedor móvil para crear la plataforma para pagos y transferencia de dinero. No obstante, en la práctica, el modelo parece prosperar en los mercados donde los organismos regulatorios se vuelven partes interesadas activas y ayudan a liderar innovaciones. Este estudio de caso demuestra que es esencial que la comunidad empresarial local adopte un enfoque holístico con respecto a los esfuerzos de defensa, y trabaje con los organismos regulatorios para determinar qué reformas promoverían mejor la innovación y el crecimiento.

Fuentes: "Innovation in Electronic Payment Adoption: The Case of Small Retailers," World Bank Group y World Economic Forum, junio de 2016. International Finance Corporation, M-Money Channel Distribution Case – Kenya. Web; Pablo Arabéhéty García. The Replication Limits of M-Pesa in Latin America. CGAP, julio de 2016; Leo Mirani. Why mobile money has failed to take off in India. Quartz junio de 2014; Anna Leach, "17 Ways to Take Your Innovation to Scale". The Guardian. Web. 18 de julio de 2014

Implementación y aplicación de regulaciones relacionadas con los pagos electrónicos

Como se indica arriba, el acceso al servicio bancario sigue siendo un considerable desafío para muchas empresas locales y consumidores, y los pagos electrónicos bancarios pueden estar sujetos a requisitos regulatorios. Si bien hay una creciente presencia de proveedores de servicios de pagos alternativos no bancarios, puede ser difícil para estos nuevos proveedores y para los organismos reguladores implementar adecuadamente las leyes para mantenerse al día con la innovación. Para asistir a las empresas y organismos reguladores, han surgido "entornos regulatorios de prueba" como una solución para explorar el rango complejo de regulaciones financieras y a la vez facilitar la aplicación. El término entorno regulatorio de prueba, creado en el RU, se refiere a un espacio legalmente seguro para que las empresas prueben nuevos productos, servicios, modelos comerciales y mecanismos de entrega sin repercusiones legales adversas.[145] Esto permite que los productos lleguen al mercado que, de otra manera, no hubiesen sido lanzados ni probados.[146] Otros beneficios de estos mecanismos incluyen un mejor acceso a servicios financieros y de pago que llegan al mercado más rápido y con costos más bajos.[147] El RU, Australia, Singapur, Hong Kong y los Países Bajos ya han implementado entornos regulatorios de prueba para promover la innovación en la industria del pago electrónico. Como se muestra en el estudio de caso a continuación, brindan oportunidades únicas para que las empresas trabajan de cerca con los organismos reguladores, no solo con respecto a cuestiones de aplicación e implementación, sino también para hacer hincapié en regulaciones particularmente difíciles y, potencialmente, para participar en el proceso de elaboración de leyes.

Estudio de caso:
Entorno regulatorio de prueba para Luno en el Reino Unido

La Autoridad Británica de Conducta Financiera (FCA, por sus siglas en inglés) fue el primer organismo regulador en adoptar entornos regulatorios de prueba para promover productos de FinTech en el mercado. La iniciativa entró en vigencia en junio de 2016 y brinda a los solicitante dos períodos de seis meses por año para probar sus productos. El objetivo principal del experimento de entornos regulatorios de prueba fue proporcionar a las empresas "acceso a experiencia regulatoria que el entorno de prueba ofrece para reducir el tiempo y el costo de llevar ideas al mercado".

Una vez que una empresa es aceptada en el entorno de prueba, se le asigna un oficial de caso de la FCA, que ayudará a diseñar el entorno de prueba para su modelo comercial. El oficial de caso también brinda orientación legal para entender las normas o regulaciones aplicables al modelo comercial de la empresa, incluso interpretaciones de los requisitos que la empresa debe cumplir. Además, para facilitar el proceso de prueba, la FCA tiene la habilidad de exonerar o modificar cualquier norma excesivamente complicada que podría obstaculizar el desempeño de la empresa en el entorno de prueba.

Un ejemplo exitoso de una compañía que usó un entorno de prueba es Luno, una nueva empresa sudafricana que desarrolló un servicio de envío de dinero transfronterizo habilitado para operar en la web. Bajo la supervisión de la FCA y en cooperación con socios bancarios, Luno probó la eficacia de enviar dinero de mercados desarrollados a mercados en desarrollo utilizando monedas digitales descentralizadas. Marcus Swanepoel, Director Ejecutivo y cofundador de Luno declaró que "Hemos trabajado de cerca con diferentes organismos reguladores en todo el mundo, y nuestra interacción con la FCA sin duda nos ayudó a mejorar nuestro entendimiento de las cuestiones regulatorias que afectan nuestro negocio".

De acuerdo con el Informe del Entorno Regulatorio de Prueba de 2017 de la FCA, aún es demasiado pronto para sacar a conclusiones de gran alcance sobre el impacto general de los entornos regulatorios de prueba. No obstante, los resultados de 2017 ya demuestran un progreso para promover la competencia e inclusión en el sector financiero. Setenta y cinco por ciento de los solicitantes iniciales en el primer año han completado con éxito la prueba, y el 90 por ciento de esos productos continuó un lanzamiento más amplio en el mercado.

Fuente: EY, As FinTech evolves, can financial services innovation be compliant? The emergence and impact of regulatory sandboxes- in the UK and across Asia-Pacific. Web. 2017; FCA, Regulatory sandbox lessons learned report. Web. Octubre de 2017; Paul Golden, Regulation and Innovation Thrive Together in The FCA's Sandbox, Euromoney. Web. 22 de febrero de 2017

Marcos institucionales relacionados con los pagos electrónicos

Otro aspecto complejo de los pagos electrónicos son los marcos institucionales complicado que existen en todo el mundo. En el nivel nacional, muchas jurisdicciones tienen una estructura de múltiples agencias. Por ejemplo, en los EE. UU., seis agencias diferentes controlan la supervisión de las instituciones de depósito, servicios de pago tradicional o basado en cuentas.[148] Otras tres agencias se ocupan de las instituciones no depositarias, como servicios de pago electrónicos no bancarios.[149] Una estructura de múltiples agencias pone más presión en las compañías para monitorear y comprender las regulaciones y pautas a veces conflictivas. Hay menos carga para las compañías cuando los organismos reguladores coordinan para emitir normas consistentes, hacen que la información sea accesible y alertan a las compañías sobre actualizaciones regulatorias a través de un amplio rango de canales, como cuentas en redes sociales o listas de correo.

Las jurisdicciones también asignan responsabilidades entre entidades nacionales y subnacionales de manera diferentes. Algunos lugares, como los EE. UU. y Canadá,[150] han delegado más responsabilidad en el nivel subnacional. Por ejemplo, los proveedores de pago no bancario deben obtener una nueva Licencia de Empresa Transmisora de Dinero en cada estado en donde el proveedor tiene pensado operar.[151] En contraste, la UE asigna gran parte de la supervisión financiera al nivel de la Unión, con el Banco Central Europeo y la Autoridad Bancaria Europa supervisando la mayoría de las supervisiones financieras. De manera similar, el Banco de Reserva de la India supervisa estrictamente las instituciones financieras que operan en el territorio.[152]

Si bien algunas jurisdicciones han establecido nuevas instituciones especializadas enfocadas en pagos electrónicos, esto todavía no es la norma. A medida que los grupos de defensa empresarial exploran las estructuras institucionales existentes, deben considerar los nuevos modelos institucionales que han surgido.

Firmas electrónicas (e-signatures)

Además de los pagos electrónicos, las firmas electrónicas son un aspecto esencial de las transacciones que se realizan en la economía digital. Las firmas manuales tradicionales son una parte establecida de la ley de contratos; sin embargo, con el surgimiento de acuerdo completamente digitales, el concepto de las firmas electrónicas presenta desafíos legales inusuales. En su forma más simple, una firma electrónica es una identidad personal basada en computadora. En los últimas décadas, las firmas electrónicas y las preocupaciones de seguridad asociadas se han vuelta cada vez más complejas, y van desde las copias electrónicas básicas de la firma manual de una persona hasta las firmas digitales que involucran a certificadores terceros.

Marcos internacionales para las firmas electrónicas

Varios marcos multilaterales y regionales son aplicables a las firmas electrónicas. En el nivel internacional, la mayoría de los esfuerzos se han realizado a través de la Comisión de las Naciones Unidas sobre la Ley de Comercio Internacional (UNCITRAL) y sus Leyes Modelo. Como el organismo jurídico central del sistema de las Naciones Unidas en la ley de comercio internacional, UNCITRAL ha promovido normas armonizadas y modernas sobre transacciones comerciales a través de una rango de iniciativas, incluso leyes y normas modelo con aceptación global.[153] Estos marcos contienen ejemplos útiles de disposiciones específicas, que los organismos reguladores y la comunidad empresarial pueden utilizan como puntos de partida útiles para la reforma o defensa. Los marcos internacionales adicionales se resumen en la **Tabla 5** a continuación. Algunas regiones, como Latinoamérica, ya han adoptado la Ley Modelo de UNCITRAL sobre Firmas Electrónicas. La adopción generalizada con el correr del tiempo podría ayudar a consolidar múltiples marcos, facilitando para las empresas de todos los tamaño operar entre fronteras. La comunidad empresarial local debe observar de cerca los desarrollos en esta área y buscar áreas donde puedan participar en el proceso de elaboración de normas siempre que sea posible.

Tabla 5. Marcos internacionales y regionales para las firmas electrónicas

Marcos	Implicaciones para la comunidad empresarial
Multilateral	
• Ley Modelo de UNCITRAL sobre el Comercio Electrónico[154] • Ley Modelo de UNCITRAL sobre Firmas Electrónicas[155]	• Las Leyes Modelo de UNCITRAL sirven como puntos de partida útiles para el debate en torno a disposiciones legales específicas sobe las firmas electrónicas. Se han utilizado como guías para informar la regulación nacional, como en una cantidad de países latinoamericanos, y podrían ser herramientas útiles para la comunidad empresarial local. • La Ley Modelo de UNCITRAL sobre el Comercio Electrónico promueve la equivalencia funcional entre los mensajes digitales y escritos, lo que equivale a un reconocimiento legal de los contratos electrónicos. También reconoce las firmas electrónicas como una manera para firmar documentos electrónico y hace hincapié en el mismo peso legal de los mensaje digitales y los documentos escritos.

	• La Ley Modelo de UNCITRAL sobre Firmas Electrónicas refleja un enfoque tecnológicamente neutral y la no discriminación de las firmas electrónicas extranjeras (las firmas electrónicas se tratan igual, y la validez de una firma electrónica depende de la confiabilidad técnica).
Regional	
• El Certificado de Origen Digital de la Asociación Latinoamericana de Integración (ALADI)[156] • Mercado Común del Sur (MERCOSUR)[157] • Código Aduanero Unificado Centroamericano (CAUCA)[158] • Zona de Libre Comercio de África Continental (AfCFTA)[159]	• Los marcos regionales para los pagos electrónicos contienen posiciones regulatorias de ejemplo que podrían informar las posiciones que la comunidad empresaria tomó a nivel nacional y con respecto a futuros acuerdos. • El Certificado de Origen Digital de la Asociación Latinoamericana de Integración apunta a una armonización gradual y aceptación de formas de firmas electrónicas. Este tipo de ley de transición podría ser adecuado para comunidades empresariales en jurisdicciones con capacidad limitada. • El MERCOSUR reconoce la validez de las firmas electrónicas dentro de toda la región, lo que facilita para la comunidad empresarial en esta región determinar los estándares de referencia; esto podría ser una buena práctica para otras regiones. • Tanto CAUCA como AfCFTA reconocen el uso de firmas electrónicas para el comercio entre sus miembros, y simplifican los requisitos para la comunidad empresarial local.

Enfoques regulatorios de las firmas electrónicas

Mientras que el reconocimiento internacional y regional de las firmas electrónicas es cada vez más común, aún hay un enfoque relativamente fragmentado con respecto a su regulación en el nivel nacional. Esto significa que las empresas que participan en comercio internacional tal vez deban considerar múltiples requisitos para garantizar la validez de sus contratos, lo que puede ser difícil para todas las compañías, excepto las más grandes. Sin embargo, existen tendencias regulatorias comunes independientemente del enfoque utilizado. Por ejemplo, la mayoría de las jurisdicciones reconocen que la validez de los contratos depende de la intención de las partes de cumplir con el acuerdo, sin importar si el contrato es escrito, electrónico o verbal. Argentina,[160] Nueva Zelanda[161] y Canadá[162] reconocen la validez de los contratos electrónicos a través de la legislación o regulación. Además de confirmar que los contratos electrónicos tienen la misma condición que los contratos tradicionales, la mayoría de las jurisdicciones ahora aceptan las firmas electrónicas en el curso del negocio regular y las consideran exigibles en un tribunal.

No obstante, muchas jurisdicciones también establecen excepciones que invalidan explícitamente ciertas categorías de firmas electrónicas. Si bien los países difieren con respecto a sus listas específicas de excepciones, suelen girar en torno a cuestiones de herencia y derecho de familia, como el divorcio.[163] Otros también excluyen procesos legales específicos, como la concesión de poder notarial en la India y la exclusión de certificación por notario en Brasil.[164] En los países latinoamericanos, si bien el uso de firmas electrónicas se reconoce ampliamente para documentos comerciales, el uso de las firmas escritas y los servicios del notario aún es obligatorio para los documentos públicos o ciertos tipos de contratos (como contratos de bienes raíces).[165] De manera similar, los jueces en el estado de California en los EE. UU. han decidido que aunque las firmas electrónicas son apropiadas en muchos entornos comerciales, no constituyen un reemplazo absoluto de las firmas originales manuales.[166]

Por esta razón, una de las preguntas más importantes que la comunidad empresarial local debe hacerse es cómo su jurisdicción define los diferentes tipos de firmas electrónicas y si se tratan diferente en virtud de las normas. Existen tres tipos principales de firmas electrónicas, que varían en el nivel de seguridad que brindan:[167]

1. **Firmas de clic para firmar:** Estas incluyen marcar casilleros, e-squiggles, imágenes escaneadas y nombres tipeados;
2. **Firmas electrónicas básicas:** El firmante aplica su firma manual a un documento de manera electrónica y el documento en general está protegido con una firma digital criptográfica propiedad de una organización proveedora de servicios que actúa como "testigo" de la firma.
3. **Firmas digitales:** Estas son el tipo más avanzado y seguro de firma. Usan una identificación digital basada en certificado emitida por una Autoridad de Certificación (CA, por sus siglas en inglés) o Proveedor de Servicios de Confianza (TSP) que vincula de forma única la firma a la identidad del firmante. En general, se utiliza una Infraestructura de Claves Públicas (PKI), un medio de autenticación y control de acceso a redes no confiables,[168] para verificar la integridad del documento.[169]

Las jurisdicciones tienden a regular las firmas electrónicas en virtud de uno de los tres enfoques regulatorios, lo que afectará cómo los diferentes tipos de firmas electrónicas se tratan en términos de su validez, legalidad y admisibilidad en un tribunal. Estos tres enfoques se ilustran en el **Diagrama 5** y se analizan a continuación.

Diagrama 5. Enfoques regulatorios sobre la firmas electrónica

Fuente: New Markets Lab (2018)

Sistemas tecnológicamente neutrales: Estas leyes o regulaciones tratan las firmas manuales y las firmas electrónicas por igual, sin importar la tecnología subyacente.[171] Algunos ejemplos de países con leyes o regulaciones tecnológicamente neutrales incluyen Australia,[172] Nueva Zelanda,[173] y Canadá.[174] Un enfoque más tecnológicamente neutral es el menos complicado para la comunidad empresarial local, alienta a las partes a celebrar contratos electrónicos y promueve la difusión de tecnologías específicas y contratos electrónicos.

Sistemas de dos niveles: Si bien estos sistemas legales también aceptan la legalidad y exigibilidad de todas las firmas electrónicas, consideran ciertos tipos de firmas electrónicas más válidas legalmente, dependiendo del nivel de seguridad provisto por sus sistemas de autenticación.[175] Algunos ejemplos de marcos con sistemas de dos niveles incluyen la UE,[176] la mayoría de los países latinoamericanos[177] y Rusia.[178]

Sistemas prescriptivos: Este enfoque es el más restrictivo y tecnológicamente específico, y no considera que todas las firmas electrónicas sean legalmente válidas. Algunos sistemas prescriptivos también imponen sanciones legales cuando una firma electrónica cae fuera de una lista específica de esquemas legales de firma electrónica.[179] Algunos ejemplos de sistemas prescriptivos incluyen India,[180] Malasia[181] y Corea del Sur. Este enfoque podría crear barreras para algunos miembros de la comunidad empresarial local y limitar nuevos tipos de firmas o tecnologías.[182]

Implementación y aplicación de las firmas electrónicas

Como a veces recae en los organismos judiciales determinar las definiciones y clasificaciones de las firmas electrónicas, los desafíos que han surgido con respecto a la implementación y aplicación tienden a estar principalmente en el sector público. En China, por ejemplo, algunos jueces son reacios en reconocer las firmas electrónicas, a pesar que la ley las reconoce claramente.[183] A medida que los responsables de elaborar políticas promulgan normas para aclarar la condición de los diferentes tipos de firmas electrónicas, los grupos de defensa empresarial deberían trabajar lo más estrechamente posible con el sector público para garantizar que se aborden sus necesidades. La comunidad empresarial local ya ha tenido éxito al trabajar con organismos reguladores en campañas dirigidas a la aplicación de las firmas electrónicas, como en el caso de Sri Lanka en la Guía Resumida. Este modelo podría ser copiado en otras jurisdicciones.

Marcos institucionales relacionados con las firmas electrónicas

El marco institucional en torno a la firma electrónica también depende de su la ley concede un valor especial a las diferentes tecnologías, y el marco regulatorio general. En las jurisdicciones tecnológicamente neutrales, el marco institucional necesario para hacer cumplir las firmas electrónicas es el mismo que el marco para las firmas tradicionales: a saber, los tribunales y los organismos de arbitraje que adjudican los contratos. Por el otro lado, muchas jurisdicciones con enfoques regulatorios específicos de tecnología, incluso los sistemas más prescriptivos y los sistemas de dos niveles, han creado un marco institucional completamente independiente para la aplicación y validación de las firmas digitales. Este marco incluye agencias gubernamentales y agentes privados.

En dichos casos, algunas relaciones e interacciones están restringidas por medio de disposiciones legales, mientras que otras están completamente vinculadas a los términos acordados en el contrato. Los agentes privados pueden actuar como organismos de certificación. Estos incluyen CA o TSP, como se mencionó arriba,[184] que son comunes en la UE y Argentina. Estos agentes privados regulados deben obtener licencias de las agencias gubernamentales, y pueden brindar servicios de certificación si cumplen con los estándares tecnológicos. Por ejemplo, la regulación sobre la Identificación Electrónica, Autenticación y Servicios de Confianza (eIDAS) de la UE requiere que un organismo de evaluación de conformidad realice una autoría de los TSP, para cumplir con los requisitos legales.[185] En Argentina, un proceso similar también presenta estándares tecnológicos, que una compañía debe cumplir para convertirse en CA.[186] Se recomienda a las comunidades empresariales locales que tomen estos servicios regulados de certificación del sector privado como ejemplo, a medida que trabajan con organismos reguladores e instituciones existentes para garantizar que se aborden adecuadamente sus necesidades.

Notas finales

1. Your Dictionary, Consumer Protection Law – Legal Definition. Web.
2. OECD, Protección del consumidor en el comercio electrónico: Recomendación de OECD, 2016. Web.
3. UNCTAD, Informe sobre la reunión Ad Hoc de expertos sobre la protección del consumidor. Web. 23 de octubre de 2012
4. UNCITRAL, Ley Modelo de UNCITRAL sobre el Comercio Electrónico con Guía para la incorporación 1996: con Artículo 5 adicional adoptado en 1998, 1999. Web.
5. Econsumer, File a Complaint. Web.
6. Comisión Europea: Regulación (EU) N.º 2017/2394, 27 de diciembre de 2017.
7. Comisión Europea, Función de ECC-Net. Web.
8. ASEAN, Declaración conjunta de los medios sobre los 48 Ministros Económicos de ASEAN, agosto de 2016. Web.
9. UNCTAD, Protección del consumidor en comercio electrónico Web. Julio de 2017; Amy J. Schmitz, Remedy Realities in Business-to-Consumer Contracting, 58 Ariz. L. Rev. 213, 246(2016)
10. Consumer Affairs Victoria, Institutional Arrangements for Consumer Protection Agencies. Web. 2008.
11. Confianza Online, Código Ético, Web
12. Toughnicke, Reglamento de Malasia y protección del consumidor de comercio electrónico y negocios en línea. Web. 6 de mayo de 2018
13. Instituto de investigación de la legislación coreana, Ley de protección del consumidor en el comercio electrónico, Etc. Web.
14. Comisión Europea, Directiva de Comercio Electrónico 2000/31/EC, Artículo 5.
15. por ejemplo, en Gales e Irlanda del Norte, los operadores de alimentos en línea deben exhibir las clasificaciones de higiene que reciben de los inspectores públicos. BBC, Los restaurantes y la comida para llevar deben exhibir las clasificaciones de higiene, LGA Says, 9 de septiembre de 2017. Web.
16. Kamal Halili Hassan, E-commerce and Consumer Protection in Malaysia: Advertisement and False Description, IPEDR Vol.32 (2012)
17. Por ejemplo, la Ley de Transacciones Comerciales Específicas y la Ley contra Primas Injustificadas y Representaciones Engañosas y sus pautas. Robert Bond, E-Commerce in 25 jurisdictions worldwide. 2010. Web.
18. Autoridad de estándares de publicidad de Singapur, Directrices sobre comunicación de marketing interactivo y redes sociales. Web. 29 de septiembre de 2016
19. Rahul Aggarwal, "A Marketer's Guide to User-Generated Content Rights and Ownership," Convince&Convert, Web. Última visita el 31 de agosto de 2018. Ver, Proyecto de Ley de Comercio Electrónico en China, Capítulo II, Sección 18, 33; Autoridad de Competencia y Mercados, Revisiones y Aprobaciones en línea. Web. Última actualización el 27 de julio de 2017.
20. OECD, Protección del consumidor en el comercio electrónico: Recomendación de OECD, 2016, Sección 5. Web.
21. Latin p.12.
22. E. Luger, T. Rodden, S. Moran, Consent for All: Revealing the Hidden Complexity of Terms and Conditions, proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013. Web.
23. OECD, Protección del consumidor en el comercio electrónico: Recomendación de OECD, 2016, Sección 25. Web.
24. Ver, por ej.: Comisión Europea, Directiva 93/13 / CEE, 5 de abril de 1993, Artículo 3.
25. UNCTAD, Manual sobre protección del consumidor, 2016.
26. UNCTAD, Protección del consumidor en comercio electrónico Web. Julio de 2017; Amy J. Schmitz, Remedy Realities in Business-to-Consumer Contracting, 58 Ariz. L. Rev. 213, 246(2016).
27. Red Aspen de Emprendedores de Desarrollo, Guía Legal del Este de África. Web.
28. Red Aspen de Emprendedores de Desarrollo, Guía Legal del Este de África. Web.
29. Your Europe, Garantías y devoluciones. Web.
30. Ley de Protección de los Derechos e Intereses de los Consumidores de la República Popular China (PRC), Sección 25.

31. ASEAN, Compendios de protección al consumidor y estudios de casos: Una guía de política (Volumen I). Web.
32. Comisión Europea, Regulación (EC) 1169/2011, Artículo 16.
33. FTC, la Ley de WEB SEGURA de EE.UU.: Los primeros tres años. Diciembre de 2009.
34. UNCTAD, Manual sobre la protección del consumidor. Web. 2016.
35. Consumer Affairs Victoria, Acuerdos institucionales para las agencias de protección del consumidor. Web. Abril de 2008.
36. Consumer Affairs Victoria, Acuerdos institucionales para las agencias de protección del consumidor. Web. Abril de 2008.
37. Ver CMA (UK), sobre nosotros. Web; FTC, sobre la FTC. Web.
38. UNCTAD, Manual sobre la protección del consumidor. Web. 2016,
39. APEC, Reunión del subgrupo de privacidad de datos con la Unión Europea. Web. 2017; Hunton Andrews Kurth, APEC and EU Discuss Interoperability Between Data Transfer Mechanisms. Web. 25 de agosto de 2017;
40. UNCTAD, Evaluación preliminar: Beneficios potenciales para las economías y las empresas de APEC que se unen al sistema CBPR. Web. Febrero de 2016.
41. Ver Mark Wu, Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange at 29, Geneva: Centro Internacional de Comercio y Desarrollo Sostenible (ICTSD) y el Banco Interamericano de Desarrollo (BID). Web. Noviembre de 2017.
42. Gobierno de Canadá, Acuerdo Integral y Progresivo para la Asociación Transpacífica (CPTPP), Web. 8 de marzo de 2018.
43. Center for International Governance Innovation, Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. Web. 4 de abril de 2018; Web.
44. OECD, Pautas de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales. Web.
45. Consejo de Europa, Convenio para la protección de las personas en relación con el procesamiento automático de datos personales. Web.
46. Gobierno de Canadá, Acuerdo Integral y Progresivo para la Asociación Transpacífica (CPTPP), Web. 8 de marzo de 2018.
47. APEC, APEC Privacy Framework. Web. Diciembre de 2015.
48. Unión Africana, Convención de la Unión Africana sobre Seguridad Cibernética y Datos Personales. Web. 14 de junio de 2014
49. Comunidad Económica de los Estados de África Occidental, Ley Complementaria de Protección de Datos de la Comunidad Económica de los Estados de África Occidental (CEDEAO). Web. 16 de febrero de 2010
50. USTR, Resumen de objetivos para la renegociación del NAFTA. Julio de 2017
51. Gobierno de Canadá, Acuerdo Integral y Progresivo para la Asociación Transpacífica (CPTPP), Web. 8 de marzo de 2018.
52. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016.
53. DLA Piper, Leyes de protección de datos del mundo: Corea del Sur. Web. 16 de enero de 2017
54. Bruno Bioni y Renator Leite Monteiro. Proyecto de ley general brasileña sobre la protección de datos personales. IAPP. Web. 31 de enero de 2018; Bill 5276/2016 Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Web.
55. Royal College of Pathologists of Australasia, Manejo de la información de privacidad en Laboratorios. Web.
56. Regulación (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en relación con el tratamiento de datos personales y sobre la libre circulación de dichos datos, y por la que se deroga la Directiva 95/46 / CE (Reglamento general de protección de datos).
57. Covington, China emite un nuevo estándar de protección de la información personal. Web. 25 de enero de 2018
58. Mengyi Wang, Data Governance in the Age of Artificial Intelligence. En preparación.
59. Egypt Today, Parliament to make firm decision on Data Protection Draft Law. Web. 18 de enero de 2018.
60. Center for International Governance Innovation, Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. Web. April 4, 2018; Albright Stonebridge Group, Localización de datos. Web. Septiembre de 2015.

61. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
62. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
63. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
64. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. 13. Web. 2016
65. Comisión Federal de Comercio, Instituciones Financieras e Información del Cliente: Cumplir con la norma de protecciones. Web.
66. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
67. Comisión de protección de datos, Registro. Web.
68. Ley de Privacidad de Australia 1998, Sección 6D.
69. DLA Piper, Leyes de protección de datos del mundo. Web.
70. DLA Piper, Leyes de protección de datos del mundo. Web.
71. DLA Piper, Leyes de protección de datos del mundo. Web.
72. Linklaters, Datos protegidos de la República Popular China. Web.
73. Conferencia Nacional de Legislaturas Estatales, Leyes de Notificación de Violación de Seguridad. Web. 29 de marzo de 2018
74. Conferencia Nacional de Legislaturas Estatales, Leyes de Notificación de Violación de Seguridad. Web. 29 de marzo de 2018
75. Regulación (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en relación con el tratamiento de datos personales y sobre la libre circulación de dichos datos, y por la que se deroga la Directiva 95/46 / CE (Reglamento general de protección de datos)
76. Proyecto de ley general brasileña sobre la protección de datos personales. Web.; Covington, China emite nuevo estándar de protección de información personal. Web. 25 de enero de 2018
77. PricewaterhouseCoopers, Portabilidad de datos de GDPR. Web.
78. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
79. Mori Hamada & Matsumoto, Amendments to the Act on the Protection of Personal Information and Relevant Issues. Web; Mengyi Wang, Data Governance in the Age of Artificial Intelligence. En preparación; Nicolas & De Vega Law Offices, Data Privacy in The Philippines. Web; Begoña Cancino, Creel, García-Cuéllar, y Aiza y Enriquez, SC, Protección de datos en México: Descripción general. Web.
80. Linklaters, Datos protegidos de la República Popular China. Web; DLA Piper, Leyes de protección de datos en el mundo. Web.
81. "Forum Shopping" se produce cuando una parte de una disputa reconoce que múltiples tribunales pueden tener jurisdicción sobre el reclamo y elige uno que tratará su reclamo más favorablemente.
82. Comisión de protección de datos, Derechos de las personas. Web.
83. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016.
84. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
85. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, reglamentos de protección de datos y flujos de datos internacionales: Implicaciones para el comercio y el desarrollo. Web. 2016
86. Mengyi Wang, Data Governance in the Age of Artificial Intelligence. En preparación.
87. UNCTAD, Evaluación preliminar: Beneficios potenciales para las economías y las empresas de APEC que se unen al sistema CBPR. Web. Febrero de 2016.
88. DLA Piper, Leyes de protección de datos del mundo. Web. Linklaters, Datos protegidos de la República Popular China. Web.
89. Unión Internacional de Telecomunicaciones, Definición de Ciberseguridad. Web.
90. Unión Internacional de Telecomunicaciones.
91. Organización para seguridad y cooperación en Europa. Cyber/ICT Security.

92. Organización de los Estados Americanos. Cyberseguridad. Web.
93. OECD, Pautas para la Seguridad de las Redes y Sistemas Informáticos: Hacia una cultura de seguridad. Web. 1 de octubre de 2015
94. National Public Radio, Brazil's Cybercrime Free-For-All: Many Scams and Little Punishment. Web. 15 de junio de 2015
95. Abusix, 2016 Rio Olympics: Brasil es el segundo generador de delitos informáticos del mundo. Web. 21 de agosto de 2017
96. Gobierno del Reino Unido. La estrategia de ciberseguridad del RU 2011-2016. Informe Anual. Web. Abril de 2016.
97. Ola Sage, Todas las pequeñas empresas deben utilizar el marco de seguridad cibernética del NIST. Web. 2015.
98. Cabinet Office, La estrategia de ciberseguridad del Reino Unido, Proteger y promover el Reino Unido en un mundo digital. Web. Noviembre de 2011.
99. Cabinet Office, La estrategia de ciberseguridad del Reino Unido, Proteger y promover el Reino Unido en un mundo digital. Web. Noviembre de 2011.
100. HM Government, Small Businesses: What You Need to Know about Cyber Security, marzo de 2015. Web.
101. Clifford Chance, Nueva legislación que regula la ciberseguridad en internet en Rusia. Web. 2 de septiembre de 2017; Organization for Economic Cooperation and Development, Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy. OECD 2012. 49; Council on Foreign Relations, The Rise of Digital Protectionism: Insights from a CFR Workshop. Web. 18 de octubre de 2017; Human Rights Watch, Vietnam: Withdraw Problematic Cyber Security Law. Web. 7 de junio de 2018.
102. Clifford Chance, Nueva legislación que regula la ciberseguridad en internet en Rusia. Web. Septiembre de 2017.
103. El gobierno federal define incidente como "un suceso que pone realmente o inminentemente en peligro, sin autoridad legal, la integridad, confidencialidad o disponibilidad de la información en un sistema de información, o que pone realmente o inminentemente en peligro, sin autoridad legal, un sistema de información" 6 USC § 148(a)(3); el Departamento de Servicios Financieros del estado de Nueva York define un evento de ciberseguridad como "un acto o intento, exitoso o no exitoso, de obtener acceso no autorizado, alterar o usar indebidamente un sistema de información o información almacenada en dicho sistema de información".
104. El Proyecto de Ley sobre Ciberseguridad de Singapur define "incidente de ciberseguridad" a un acto o actividad a través de una computadora o sistema informático que puso en peligro o afectó negativamente, sin autoridad legal, la seguridad, disponibilidad o integridad de una computadora o sistema informático, o la disponibilidad, confidencialidad o integridad de la información guardada, procesada o transmitida en una computadora o sistema informático.
105. Ley de ciberseguridad de 2015.
106. Lexology, Seguridad de los datos y delitos informáticos en Rusia. Web. 12 de marzo de 2018
107. Ponemon Institute. 2017 Estado de ciberseguridad en pequeñas y medianas empresas (SMB). Web. Septiembre de 2017.
108. Karl Flinders, Las PyMEs del RU tienen un sentido falso de la ciberseguridad. Web. 13 de septiembre de 2016
109. Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.
110. Este monto de referencia incluye una defensa perimetral, como usar firewalls de red e instalar protección contra malware de nivel empresarial en todas las computadoras que se utilizan como parte de la compañía. El personal de ICT también debe manejar las vulnerabilidades de seguridad y mantener los sistemas actualizados con el software más reciente. Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.
111. Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.
112. Agencia de la Unión Europea para la Seguridad de las Redes y la Información. Seguridad de la información y estándares de privacidad para las PyMEs: Recomendaciones para mejorar la adopción de la seguridad de la información y estándares de privacidad en pequeñas y medianas empresas. Web. Diciembre de 2015. 15.
113. Agencia de la Unión Europea para la Seguridad de las Redes y la Información. Seguridad de la información y estándares de privacidad para las PyMEs: Recomendaciones para mejorar la adopción de la seguridad de la información y estándares de

privacidad en pequeñas y medianas empresas. Web. Diciembre de 2015. 19.

114. Agencia de la Unión Europea para la Seguridad de las Redes y la Información. Seguridad de la información y estándares de privacidad para las PyMEs: Recomendaciones para mejorar la adopción de la seguridad de la información y estándares de privacidad en pequeñas y medianas empresas. Web. Diciembre de 2015. 15.

115. DLA Piper, International Cybersecurity Standards: Practical Applications for Growing Corporate Value. Web. 12 de septiembre de 2016

116. Instituto Nacional de Estándares y Tecnología. Marco para mejorar la ciberseguridad de infraestructura crítica – Versión 1.1. 16 de abril de 2018

117. Centro para la seguridad en internet. Controles CIS. Web.

118. allAfrica, Mauritius ranks 1st on 2017 Global Cybersecurity Index in Africa. Web. Junio de 2018. 2017.

119. Unión Internacional de Telecomunicaciones. "Global Cybersecurity Index 2017." 2017. 4.

120. Equipo de Respuesta ante Incidentes de Seguridad Informática del Sector Financiero de Sri Lanka. Web.

121. August Pons, Mengzhen Wang y Lauren Sillman, Regulatory Burdens on MSMEs and E-Commerce in Lebanon, TradeLab, 2018.

122. European Parliament, Financial Services Liberalization and TiSA: implications for EU Free Trade Agreements. Web. Julio de 2016.

123. Banco Mundial. Iniciativa global de inclusión financiera. Web.

124. World Bank, Global Findex Database 2014: Measuring Financial Inclusion around the World. Web. 15 de abril de 2015

125. World Bank, Payment Aspects of Financial Inclusion. Web. Abril de 2016.

126. Ley Nacional de Protección del Crédito del Consumidor de 2009 (Ley Nacional de Crédito).

127. Ley del Banco de Infraestructura del Mercado Financiero (FMIA) Art. 81

128. New Markets Lab/World Economic Forum, The Role of Law and Regulation in International Trade Finance: The Case of Correspondent Banking. Web. Julio de 2017.

129. Estándares internacionales sobre la lucha contra el lavado de dinero y la financiación del terrorismo y la proliferación, Grupo de acción financiera, 2012.

130. Ley Nº 5476 de 2015 de Paraguay.

131. Circular 29/2008 publicada en el Diario Oficial de la Federación el 11 de julio de 2008.

132. Regulación (UE) 2015/751 del Parlamento Europeo y del Consejo, de 29 de abril de 2015, sobre tasas de intercambio para transacciones con pago con tarjeta, Artículo 12.

133. Por ejemplo, la UE ha limitado la tarifa de tarjeta de débito a 0.2 por ciento del valor de una transacción y la tarifa de tarjeta de crédito a 0.3 por ciento del valor de una transacción, Regulación (UE) 2015/751 del Parlamento Europeo y el Consejo del 29 de abril de 2015 Tasas de intercambio para transacciones con pagos basados en tarjeta Artículos 3 y 4.

134. Colombia Ley 1480 de 2011

135. Ley 25.065 de 1998 de Argentina.

136. Ley de Protección del Consumidor, No. 46 of 2012.

137. Manejo de IT, los 12 requisitos de PCI DSS. Web.

138. Mastercard, What service providers need to know about PCI compliance. Web, Jacqueline Von Ogden, How Much Does PCI Compliance Cost? 9 Factors to Consider. Web. 24 de marzo de 2016

139. Incluyen Argentina, Columbia, la UE, Kenia y los EE. UU., entre otros. Ver Ley 25.065 de 1998; Colombia Ley 1480 de 2011; Establécense normas que regulan diversos aspectos vinculados con el sistema de Tarjetas de Crédito, Compra y Débito. Relaciones entre el emisor y titular o usuario y entre el emisor y proveedor. Disposiciones Comunes. Web; Ley de Protección del Consumidor, No. 46 of 2012.

140. PSD2 para (71) and Chapter 6; Fair Credit Billing Act. 15 USC 160; Fair Credit Billing Act. 15 USC 160.

141. John Rampton, Accepting Credit Cards 101: What Your Business Needs to Know. Web. Enero de 2017.

142. Industria de Tarjeta de Pago, Guía de cumplimiento. Web.

143. Ley de sistemas de pago y liquidación de la India de 2007, Capítulo III.

144. Marianne Crowe, Mary Kepler y Cynthia Merrit, The U.S. Regulatory Landscape for Mobile Payments: Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators on April 24, 2012. Web. Julio de 2012.

145. Autoridad de Conducta Financiera (FCA), Entorno Regulatorio de Prueba, Web. Noviembre de 2015.

146. Capgemini. Top 10 Trends in Payments 2017: What you need to know. Web. 2017.

147. FCA, Entorno Regulatorio de Prueba, Web. Noviembre de 2015.
148. U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Banks and Credit Unions. Web. Junio de 2017.
149. U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Banks and Credit Unions. Web. Junio de 2017.
150. STI, Starting a financial institution in Canada, Web.
151. Cada estado ha adoptado leyes que regulan las Licencias de Empresa Transmisora de Dinero, una tabla comparativa disponible en: Thomas Brown, 50-State Survey: Money Transmitter Licensing Requirements. Web.
152. The Banking Regulation Act, 1949.
153. UNCITRAL, About UNCITRAL. Web.
154. Sin embargo, estos instrumentos no son vinculantes, a menos que el país signatario decida adoptarlos como tal. La Secretaría de UNCITRAL confirma que, hasta ahora, 32 estados tienen legislación basada o influida por la Ley Modelo.
155. Ley Modelo de UNCITRAL sobre Firma Electrónica; UNCITRAL, Guía para la promulgación de la Ley Modelo de UNCITRAL sobre Firmas Electrónicas.
156. Argentina, Bolivia, Brasil, Chile, Cuba, Colombia, Ecuador, México, Panamá, Paraguay, Perú, Uruguay, y Venezuela
157. Argentina, Brasil, Uruguay y Paraguay
158. Costa Rica, República Dominicana, El Salvador, Honduras, Guatemala y Panamá han adoptado el Código Aduanera Unificado Centroamericano.
159. Acuerdo firmado por 44 países africanos para crear una Zona de Libre Comercio de África Continental.
160. Sección 1017 del Código Civil y Comercial.
161. Ley de Transacciones Electrónicas 2002.
162. Ley de Comercio Electrónico Uniforme (1999).
163. Por ejemplo, la República Checa excluye ciertos tipos de firmas electrónicas en documentos relacionados con el derecho de sucesiones. Sección 1582 (2) del Código Civil), ventas de sucesión (Sección 1714 (3) del Código Civil), renuncia del derecho de sucesión (Sección 1484 del Código Civil)
164. DocuSign, eSignature Legality Guide, Web.
165. DocuSign, eSignature Legality Guide, Web.
166. United States Bankruptcy Court Central District of California, New Local Bankruptcy Rule 9011-1, en vigencia el 1 de diciembre de 2017.
167. SigningHub. Electronic Signatures: Understanding the Different Levels and Types. Web.
168. Hongkong Post e-Cert, Concepts of PKI. Web.
169. Adobe, Adobe Sign - Digital Signature FAQs. Web.
170. Adobe, Adobe Sign - Digital Signature FAQs. Web.
171. SigningHub. Electronic Signatures: Understanding the Different Levels and Types. Web.
172. Regulaciones de Transacciones Electrónicas 2000.
173. Ley de Transacciones Electrónicas 2002.
174. Ley de Comercio Electrónico Uniforme (1999).
175. OASIS PKI, Leyes y regulaciones de firmas electrónicas. Web.
176. La Regulación Nº910/2014 de la Unión Europea.
177. DocuSign, eSignature Legality Guide. Web.
178. Ley Federal de la Federación Rusa No. 63-FZ sobre firmas electrónicas 2011.
179. Ley Federal de la Federación Rusa No. 63-FZ sobre firmas electrónicas 2011.
180. Ley de Tecnología de la Información 2000.
181. Ley de Firma Digital 1997.
182. El enfoque prescriptivo de Corea del Sur ha resultado en que las empresas mantienen sistemas de autenticación obsoletos. El caso de Corea del Sur y su tecnología de compensación de transacciones financieras es un buen ejemplo de los efectos que puede tener un sistema regulatorio prescriptivo para las firmas electrónicas. Scott J. Shackelford, Scott Russell y Jeffrey Haut, Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks. Web. 2016.
183. DocuSign, eSignature Legality Guide, Web.
184. La Regulación Nº910/2014 de la Unión Europea.
185. Sección 3 de la Regulación Nº910/2014 de la Unión Europea.
186. Ley de Argentina 25506 Firma digital.