



2020

Políticas para la  
**economía digital**  
en Costa Rica

Publicado originalmente por la OCDE bajo el título: OCDE (2020), *Digital Economy Policy in Costa Rica*, disponible en el sitio web <https://www.oecd.org/countries/costarica/digital-economy-policy-in-costa-rica.pdf>. La OCDE tiene dos idiomas oficiales: inglés y francés. La versión en inglés de este informe es la única oficial. Traducido por el Gobierno de Costa Rica. La calidad de la traducción, su contenido técnico y coherencia con la versión oficial es responsabilidad única y exclusiva del Gobierno de la República de Costa Rica.

## Prólogo

El presente informe, *Políticas para la economía digital en Costa Rica*, fue elaborado en noviembre de 2017 por la Secretaría de la OCDE como documento de antecedentes para el examen de adhesión de Costa Rica realizado por el Comité de Políticas para la Economía Digital.

El 9 de abril de 2015 el Consejo de la OCDE decidió iniciar discusiones con Costa Rica sobre su posible adhesión. El 8 de julio de 2015 el Consejo adoptó una Hoja de ruta para la adhesión de Costa Rica al Convenio de la OCDE [C(2015)93/FINAL] (la Hoja de ruta). La Hoja de ruta establece los términos, las condiciones y el proceso para la adhesión. La Hoja de ruta estipula que, con el fin de que el Consejo pueda tomar una decisión informada acerca de la adhesión de Costa Rica, los 22 comités técnicos de la OCDE someterán a Costa Rica a exámenes exhaustivos, y el Comité de Políticas para la Economía Digital es uno de ellos.

El Comité de Políticas para la Economía Digital acordó, de conformidad con el párrafo 14 de la Hoja de ruta de Costa Rica, desclasificar este Informe y publicarlo bajo la autoridad del Secretario General para que un público más amplio pudiera conocer su contenido. La publicación de este Informe y los análisis y recomendaciones que contiene no constituyen en modo alguno un juicio anticipado de los resultados del examen de Costa Rica realizado por el Comité de Políticas para la Economía Digital u otros comités técnicos como parte del proceso de adhesión de Costa Rica a la OCDE.

Karine Perset de la División de Políticas para la Economía Digital de la Dirección de Ciencia, Tecnología e Innovación (STI por sus siglas en inglés) de la OCDE llevó a cabo la revisión, con la asistencia de Tais Niffneger, Graham Vickery, Laurent Bernat, Lorryne Porciuncula, David Gierten y Anne Carblanc, todas ellas de la STI. El autor desea agradecer especialmente a Gallia Daor y Natalie Limbasan, de la Dirección Jurídica, por su gran apoyo durante todo el proceso del examen de adhesión. El informe se benefició enormemente de los aportes y comentarios del Viceministro Edwin Estrada, Francisco Troyo, Alejandro Zúñiga Mariana del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y de Marianne Bennett del Ministerio de Comercio Exterior de Costa Rica (COMEX). No podemos mencionar a la gran cantidad de personas que participaron, pero el informe se benefició enormemente de las conversaciones con muchos otros funcionarios gubernamentales y partes interesadas que compartieron generosamente su tiempo y sus opiniones con la Secretaría durante la misión a Costa Rica.

*Nota para las delegaciones:*

*Este documento también está disponible en O.N.E. bajo el código de referencia: DSTI/CDEP/ACS(2017)1/FINAL*

Este documento, así como los datos y mapas que incluye, se presenta sin perjuicio del estado o la soberanía de cualquier territorio, de la delimitación de fronteras y límites internacionales y del nombre de cualquier territorio, ciudad o área.

@ OECD 2020

Puede copiar, descargar o imprimir contenido de la OCDE para su propio uso, y puede incluir extractos de publicaciones, bases de datos y productos multimedia de la OCDE en sus propios documentos, presentaciones, blogs, sitios web y materiales didácticos, siempre que incluya el reconocimiento a la OCDE como fuente y propietario de los derechos de autor. Todas las solicitudes de uso comercial y derechos de traducción deben enviarse a [rights@oecd.org](mailto:rights@oecd.org).

## *Contenido*

<b>INTRODUCCIÓN.....</b>	<b>4</b>
<b>1. PRINCIPIOS PARA LA CREACIÓN DE POLÍTICAS DE INTERNET .....</b>	<b>6</b>
<b>2. DESARROLLO DE BANDA ANCHA.....</b>	<b>11</b>
<b>3. ITINERANCIA MÓVIL INTERNACIONAL.....</b>	<b>18</b>
<b>4. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL.....</b>	<b>20</b>
<b>5. PROTECCIÓN DE LA INFRAESTRUCTURA DE INFORMACIÓN CRÍTICA .....</b>	<b>26</b>
<b>6. CRIPTOGRAFÍA.....</b>	<b>28</b>
<b>7. AUTENTICACIÓN ELECTRÓNICA.....</b>	<b>31</b>
<b>8. SPAM.....</b>	<b>35</b>
<b>9. DECLARACIONES SOBRE LA INTERNET Y LA ECONOMÍA DIGITAL.....</b>	<b>38</b>
<b>10. INFORMACIÓN DEL SECTOR PÚBLICO .....</b>	<b>42</b>
<b>11. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) Y EL MEDIO AMBIENTE.....</b>	<b>52</b>
<b>12. PRIVACIDAD .....</b>	<b>60</b>
<b>13. LA GOBERNANZA DE DATOS DE SALUD.....</b>	<b>66</b>
<b>14. LA PROTECCIÓN EN LÍNEA DE LOS NIÑOS Y NIÑAS .....</b>	<b>69</b>

## INTRODUCCIÓN

De conformidad con la Hoja de ruta para la adhesión de Costa Rica [C(2015)93/FINAL], se le solicitó al Comité de Políticas para la Economía Digital (CDEP por sus siglas en inglés) que llevara a cabo un estudio exhaustivo de Costa Rica con el fin de proporcionar una evaluación de la disposición y la capacidad de Costa Rica para implementar los instrumentos jurídicos fundamentales de la OCDE dentro de la competencia del CDEP, y una evaluación de las políticas y las prácticas de Costa Rica en comparación con las mejores políticas y prácticas de la OCDE en el área de las políticas para la economía digital. En consecuencia, la revisión hace referencia a los Principios Básicos del CDEP definidos en el Apéndice de la Hoja de Ruta:

- Desarrollar políticas efectivas para ayudar a la expansión de la economía de internet, incluidas políticas para estimular el uso de internet, promover el desarrollo de aplicaciones, promover mercados de comunicaciones competitivos y acuerdos de suministro eficientes e innovadores.
- Cumplir los Principios de la OCDE para la formulación de políticas de internet, que exhortan a preservar la naturaleza abierta y descentralizada de la internet para estimular la innovación, brindar beneficios económicos y sociales y dar voz a las aspiraciones democráticas.
- Mejorar el acceso a la información del sector público y aumentar su uso a través de la maximización de su disponibilidad y el establecimiento de condiciones transparentes para su reutilización.
- Proteger los datos personales de los individuos y cooperar en la aplicación de las leyes de privacidad, de acuerdo con las Recomendaciones pertinentes de la OCDE.
- Promover una cultura de gestión de los riesgos de seguridad en el uso de sistemas y redes de información y proteger las infraestructuras de información crítica, incluido el desarrollo de políticas y prácticas para enfrentar estos riesgos.

En consecuencia, este informe ofrece una perspectiva general de las políticas para la economía digital en Costa Rica. Las catorce secciones de este informe están estructuradas por las áreas temáticas de los instrumentos jurídicos de la OCDE en el campo de las políticas para la economía digital. Cada sección presenta información relevante sobre políticas, instituciones responsables, el marco jurídico y regulatorio, las medidas de implementación y aplicación de la ley, y el monitoreo y evaluación de las políticas. El informe también aporta las valoraciones y recomendaciones del CDEP al final de cada sección.

La información utilizada en este informe fue recopilada a través de un cuestionario de políticas, las presentaciones de Costa Rica en las reuniones del CDEP del 16 de noviembre de 2016 y el 19 de mayo de 2017, las entrevistas realizadas a funcionarios del gobierno costarricense y representantes del sector privado y la sociedad civil durante la misión de investigación de la Secretaría en San José, Costa Rica, en enero de 2017, así como de información adicional presentada por Costa Rica desde entonces.

Las revisiones de las políticas de Costa Rica en las áreas de los principios para la formulación de políticas de internet (Sección 1), el desarrollo de banda ancha (Sección 2), los servicios de itinerancia (*roaming*) móvil internacional (Sección 3), la gestión de riesgos de seguridad digital (Sección 4), la infraestructura de información crítica (Sección 5), las firmas y la autenticación electrónicas (Sección 6), la criptografía (Sección 7) y el spam (Sección 8) fueron discutidas el 19 de mayo de 2017 por el Comité de Políticas para la Economía Digital en su 74ª sesión. Se han actualizado para incluir la información y las cifras más recientes suministradas por Costa Rica. Las revisiones de las políticas de Costa

Rica en las áreas del futuro de la economía de internet (Sección 9), la información del sector público (Sección 10), las TIC y el medio ambiente (Sección 11), la privacidad (Sección 12), la gobernanza de los datos de salud (Sección 13) y la protección en línea de los niños y las niñas (Sección 14) fueron discutida por el Comité el 22 de noviembre de 2017 en su 75ª sesión.

## 1. PRINCIPIOS PARA LA CREACIÓN DE POLÍTICAS DE INTERNET

Esta sección se centra en una selección de principios de la Recomendación del Consejo sobre los Principios relativos a la formulación de políticas de internet (PPI) (se excluyen los que se abordan en otras secciones de este informe); en particular:

- Promover y proteger el flujo libre y global de la información (Principio 1)
- Promover la naturaleza abierta, distribuida e interconectada de la internet (Principio 2)
- Promover y permitir la prestación de servicios a través de fronteras (Principio 4)
- Fomentar la cooperación de múltiples partes interesadas en los procesos de formulación de políticas (Principio 5)
- Impulsar los códigos de conducta desarrollados voluntariamente (Principio 6)
- Garantizar la transparencia, el proceso justo y la rendición de cuentas (Principio 8)
- Limitar la responsabilidad de los intermediarios de internet (Principio 12)

### 1.1. Políticas

Costa Rica se adhirió a la Recomendación del Consejo sobre los Principios relativos a la formulación de políticas de internet [[OCDE/LEGAL/0387](#)] el 11 de octubre de 2012. En su posición oficial, el gobierno costarricense apoya una internet abierta y libre y promueve el modelo de gobernanza de internet de múltiples interesados, tanto a escala nacional como internacional. El Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021 de Costa Rica es el documento principal de política estratégica en las áreas que abarcan los PPI. Contiene como objetivo específico el desarrollo de una hoja de ruta para consolidar aún más el modelo existente de gobernanza de la internet de Costa Rica con base en la participación de múltiples partes interesadas.

El Plan Nacional de Desarrollo "Alberto Cañas Escalante" 2015-2018 (PND), que es más amplio, aspira a promover una cultura nacional de ética, transparencia y responsabilidad (en el tercer pilar) que es relevante para el Principio 8 de los PPI, referente a transparencia, proceso justo y responsabilidad. El PND relaciona la transparencia, entre otras cosas, con el acceso a la información pública, acceso que se facilita mediante la implementación de un modelo de gobierno abierto que les permite a los ciudadanos costarricenses desarrollar una relación con el gobierno más estrecha y sujeta a auditorías.

#### ***Responsabilidades y facultades***

El Viceministro de Telecomunicaciones del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) lidera el desarrollo y la implementación de políticas en muchas de las áreas que abarcan los PPI.

El Ministerio de Comercio Exterior (COMEX) negocia acuerdos comerciales para Costa Rica y participa en todas las discusiones nuevas sobre el comercio transfronterizo de servicios con el fin de garantizar mercados competitivos y libres.

La Superintendencia de Telecomunicaciones (SUTEL) es responsable de implementar políticas en algunas de las áreas relacionadas con los PPI y apoya al MICITT en la propuesta de políticas en algunas áreas.

El Viceministro de Asuntos Políticos y Diálogo Ciudadano del Ministerio de la Presidencia lidera el esfuerzo de promover principios de gobierno abierto en la administración pública de Costa Rica.

Las ONG, incluidas partes interesadas privadas, participan en el proceso de formulación de políticas en Costa Rica y todos los proyectos de documentos de políticas deben pasar por un proceso de consulta pública.

El Consejo Consultivo de Internet de Costa Rica, compuesto por múltiples partes interesadas y creado en 2012 por iniciativa de la comunidad técnica de internet en el país, constituye un foro para los debates sobre la gobernanza de la internet en Costa Rica.

### ***Marco jurídico y regulatorio***

#### ***Promover y proteger el flujo libre y global de la información (Principio 1)***

La Constitución de Costa Rica garantiza la libertad de expresión, opinión y comunicación; el derecho de asociarse, reunirse, presentar solicitudes al gobierno y obtener pronta resolución; y los derechos fundamentales establecidos en los instrumentos internacionales de derechos humanos. La Sala Constitucional de Costa Rica declaró que el acceso a tecnologías como la internet es un derecho fundamental de los ciudadanos que les permite ejercer sus derechos humanos (Decisión N° 10627, 2010). La decisión relaciona la internet con el derecho a la información y la comunicación, entendido como el derecho de todas las personas a acceder y participar en la producción, el intercambio y el libre flujo de la información y el conocimiento, y convierte el acceso a la red y su contenido en un requisito fundamental que abarca a toda la población de Costa Rica.

Pueden imponerse restricciones legales al libre flujo de la información en relación con los derechos a la privacidad y al secreto de las comunicaciones que establece la Constitución (Artículo 24) y la Ley N° 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales de 2011.

#### ***Promover la naturaleza abierta, distribuida e interconectada de la internet (Principio 2)***

Costa Rica apoya la neutralidad de la red, pero todavía no ha elaborado normas y reglamentos específicos en esta materia. La Ley N° 8660 de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones de 2008 contiene los principios relevantes para la neutralidad de la red; por ejemplo, obliga a los operadores a proveer acceso abierto a la red y los servicios (Artículo 75). La ley promueve la inversión en el sector de las telecomunicaciones a través de un marco jurídico que garantiza la transparencia, la no discriminación, la igualdad y la seguridad jurídica (artículo 2). Los principios rectores de la ley incluyen la no discriminación entre servicios de telecomunicaciones iguales o similares de operadores, proveedores o usuarios públicos o privados (Artículo 3).

#### ***Fomentar la cooperación de múltiples partes interesadas en los procesos de formulación de políticas (Principio 5)***

El Decreto Ejecutivo de 2015 sobre la constitución de equipos técnicos mixtos para apoyar al rector de las telecomunicaciones en los eventos de representación internacional (N° 37029-MINAET) apoya el modelo de múltiples interesados en la formulación de políticas costarricenses y la representación internacional.

*Garantizar la transparencia, el proceso justo y la rendición de cuentas (Principio 8)*

En 2012, Costa Rica se unió a la Alianza para el Gobierno Abierto, una iniciativa multilateral cuyo objetivo es asegurar compromisos concretos de los gobiernos para promover la transparencia, empoderar a los ciudadanos y combatir la corrupción. Mediante la promulgación del Decreto Ejecutivo N° 38994-MP-PLAN-MICIT en 2015, Costa Rica estableció una Comisión Nacional por un Gobierno Abierto con el objeto de "*fomentar los principios del Gobierno Abierto en la Administración Pública de Costa Rica, principios que se manifiestan en: mejorar los niveles de transparencia, garantizar el acceso democrático a la información pública, promover y facilitar la participación ciudadana e impulsar la generación de espacios de trabajo colaborativo interinstitucional y ciudadano; mediante la innovación y aprovechando al máximo las facilidades que brindan las Tecnologías de la Información y Comunicación (TIC)*".

*Impulsar los códigos de conducta desarrollados voluntariamente (Principio 6).  
Limitar la responsabilidad de los intermediarios de internet (Principio 12)*

En el área de los derechos de autor, Costa Rica promulgó el "Reglamento sobre la limitación a la responsabilidad de los proveedores de servicios por infracciones a Derechos de Autor y Conexos de Acuerdo con el Artículo 15.11.27 del Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos" (Decreto Ejecutivo N° 36880-COMEX-JP) en 2011. Este Decreto Ejecutivo establece limitaciones a la responsabilidad de los intermediarios de internet por violaciones de derechos de autor o derechos relacionados que no estén bajo su control o que no han sido iniciados o dirigidos por ellos, y que se producen a través de sistemas o redes controlados u operados por ellos o en su nombre. Además, en la Asamblea Legislativa también se está proponiendo un proyecto de ley sobre servicios de la sociedad de la información (N° 19.012). Inspirado por la Directiva Europea sobre Comercio Electrónico, su objetivo es crear un marco para los servicios electrónicos mediante la definición y la regulación de las comunicaciones electrónicas, los proveedores de servicios, la responsabilidad de los intermediarios y la promoción de códigos de conducta.

**1.2. Implementación***Promover y proteger el flujo libre y global de la información (Principio 1)*

Costa Rica apoya la libertad de expresión y la apertura y el libre flujo de información en la internet dentro de un marco de acción que garantice la privacidad y la seguridad de los usuarios. Las acciones de Costa Rica que ilustran el apoyo a una internet libre y abierta incluyen:

- La adhesión de Costa Rica a la Freedom Online Coalition (Coalición Libertad en Línea) en 2012, un grupo interregional de 29 gobiernos que colaboran para promover la libertad de la internet en todo el mundo. Costa Rica fue sede de la Conferencia Ministerial de 2016 de la Coalición Libertad en Línea.
- La decisión de Costa Rica de no firmar el Reglamento Internacional de Telecomunicaciones (ITR por sus siglas en inglés) durante la reunión del WCIT en Dubai en diciembre de 2012.

*Conectividad (relacionada con el Principio 2)*

La internet de Costa Rica está bien conectada a redes internacionales sin restricciones legales o regulatorias de conexión. Costa Rica está conectada por tres cables submarinos redundantes de fibra óptica que conectan el país a la red mundial de internet: Arcos (Océano Atlántico), Maya-1 (Océano Atlántico), y el Level 3 Communication Pan-American Crossing (Océano Pacífico). Desde abril de 2014 Costa Rica ha tenido un Punto de Intercambio de Internet (IXP) neutral llamado CRIX. El IXP, que el gobierno declaró como

un proyecto de interés público a través del MICITT, cuenta con el soporte y la gestión del Network Information Centre de Costa Rica (NIC-CR).

*Fomentar la cooperación de múltiples partes interesadas en los procesos de formulación de políticas (Principio 5)*

El Network Information Center de Costa Rica (NIC Costa Rica), que administra el dominio de nivel superior (ccTLD) para el código de país .cr, creó el *Consejo Consultivo de Internet de Costa Rica* en 2012. El Consejo Consultivo fomenta la cooperación interdisciplinaria entre múltiples interesados en los procesos de formulación de políticas. Los representantes de todos los grupos interesados –del sector privado, el gobierno, la academia y la sociedad civil– participan y proponen políticas a NIC Costa Rica sobre el desarrollo de la internet, la gobernanza de internet, el acceso universal y otros asuntos relacionados con las operaciones de la internet.

Costa Rica ha apoyado el modelo de gobernanza de la internet entre múltiples interesados a escala internacional. Por ejemplo, Costa Rica reafirmó esta posición durante la 43ª reunión de la Corporación para la Asignación de Nombres y Números de Internet (ICANN 43) en San José, Costa Rica en 2012; en la Conferencia Mundial de Telecomunicaciones Internacionales (CMTI) de la Unión Internacional de Telecomunicaciones (UIT) celebrada en Dubai en 2012; en las reuniones de los Foros para la Gobernanza de Internet (FGI) en 2013-2016; y en reuniones recientes de la Coalición Libertad en Línea (CLL).

El enfoque del desarrollo de políticas entre múltiples partes interesadas tiene especial importancia en el sector de ciencia, tecnología y telecomunicaciones de Costa Rica. Las políticas propuestas en estas áreas se discuten con representantes de los sectores público y privado (cámaras de telecomunicaciones) en reuniones y talleres, y posteriormente son objeto de consultas públicas (publicada en el diario oficial *La Gaceta*) en las que la sociedad civil puede expresar sus opiniones, hacer recomendaciones, etc. Los enfoques de múltiples interesados también se utilizan con frecuencia en la implementación de políticas. Por ejemplo, el programa de Comunidades Conectadas del PNDD incluyó consultas con las comunidades afectadas.

### 1.3. Seguimiento y evaluación

El MICITT lleva a cabo diversas actividades de monitoreo sobre temas relacionados con los PPI. Por ejemplo, monitorea los comentarios que recibe sobre proyectos de regulación, el volumen de tráfico del IXP y las entidades conectadas a él, la retroalimentación del Consejo Consultivo de Internet de Costa Rica y los avances internacionales en temas como la gobernanza de internet y el libre flujo de información.

### 1.4. Evaluación

***Recomendación del Consejo sobre los Principios relativos a la formulación de políticas de internet [OECD/LEGAL/0387]***

Costa Rica se adhirió a la Recomendación del Consejo sobre los Principios relativos a la formulación de políticas de internet [OCDE/LEGAL/0387] el 11 de octubre de 2012. Las políticas desarrolladas e implementadas por Costa Rica en las áreas que abarcan los PPI promueven el flujo libre y global de información a través de una internet abierta, distribuida e interconectada y con prestación transfronteriza de servicios. Fomentan la transparencia, el proceso justo y la rendición de cuentas, alientan el desarrollo de políticas entre múltiples interesados y trabajan por limitar la responsabilidad civil de los intermediarios de Internet en el área de los derechos de autor.

Costa Rica apoya una internet abierta y descentralizada tanto a escala nacional como internacional. La apertura de internet es fundamental para los esfuerzos de Costa Rica por fomentar el debate social y la participación civil en la formulación de políticas a través de

internet, y Costa Rica cuenta con procesos de múltiples interesados bien desarrollados. Los beneficios económicos y sociales son objetivos centrales del Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 (PNDT) de Costa Rica. Las políticas para la economía digital de Costa Rica también contribuyen a implementar el derecho constitucional a la libertad de expresión y la difusión de pensamientos y opiniones.

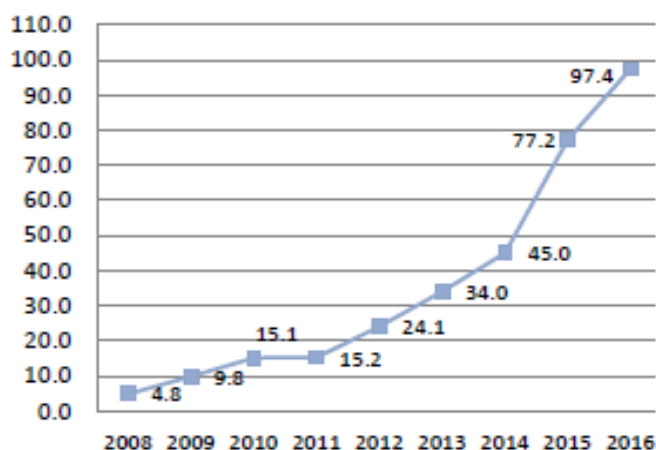
## 2. DESARROLLO DE LA BANDA ANCHA

### 2.1. Políticas

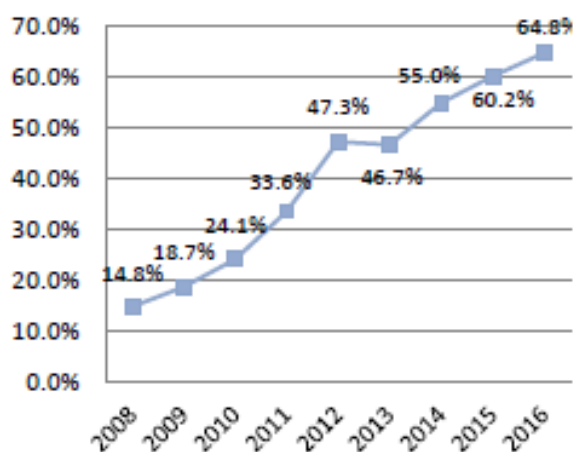
El Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 (PNDT): "Costa Rica: una sociedad conectada" establece el plan para transformar a Costa Rica en una sociedad conectada mediante el fomento de la inversión en redes y el desarrollo del acceso universal. Se basa en la Estrategia Nacional de Banda Ancha de Costa Rica de 2009, que fue implementada hasta 2014 y estableció los objetivos y modelos para el desarrollo de la banda ancha en Costa Rica. Los objetivos del PNDT relacionados con la banda ancha son: i) mejorar la calidad de la banda ancha fija y móvil a fin de proporcionar, para 2021, acceso a internet al 80% de la población a la velocidad media de los miembros de la OCDE, y ii) extender y mejorar la conectividad de banda ancha en áreas desatendidas y no rentables, especialmente mediante la ampliación de la infraestructura de banda ancha y el acceso a centros comunitarios y órganos gubernamentales.<sup>1</sup>

En los últimos años la población costarricense con acceso a internet ha aumentado drásticamente. Las suscripciones a internet aumentaron de 4.8 suscriptores por 100 habitantes en 2008 a más de 97.4 en 2016 (Figura 1). El acceso a internet fijo y móvil de los hogares también ha mejorado drásticamente, de menos del 15% de los hogares con acceso a Internet en 2008 a más del 64.8% en 2016 (Figura 2). La penetración de la banda ancha móvil en Costa Rica también fue alta en comparación con el promedio de América Latina y el Caribe (ALC) de 34.2% y el promedio de la OCDE, de 72%, llegando a 86.9% en 2014 (Figura 3). Con un 10.4% en 2014, la penetración de la banda ancha fija fue mayor que el promedio de ALC del 10%, pero considerablemente menor que el promedio de la OCDE de 28.2% (Figura 4).

**Figura 1. Suscripciones a internet (fija y móvil), por 100/hab, 2008-2016**

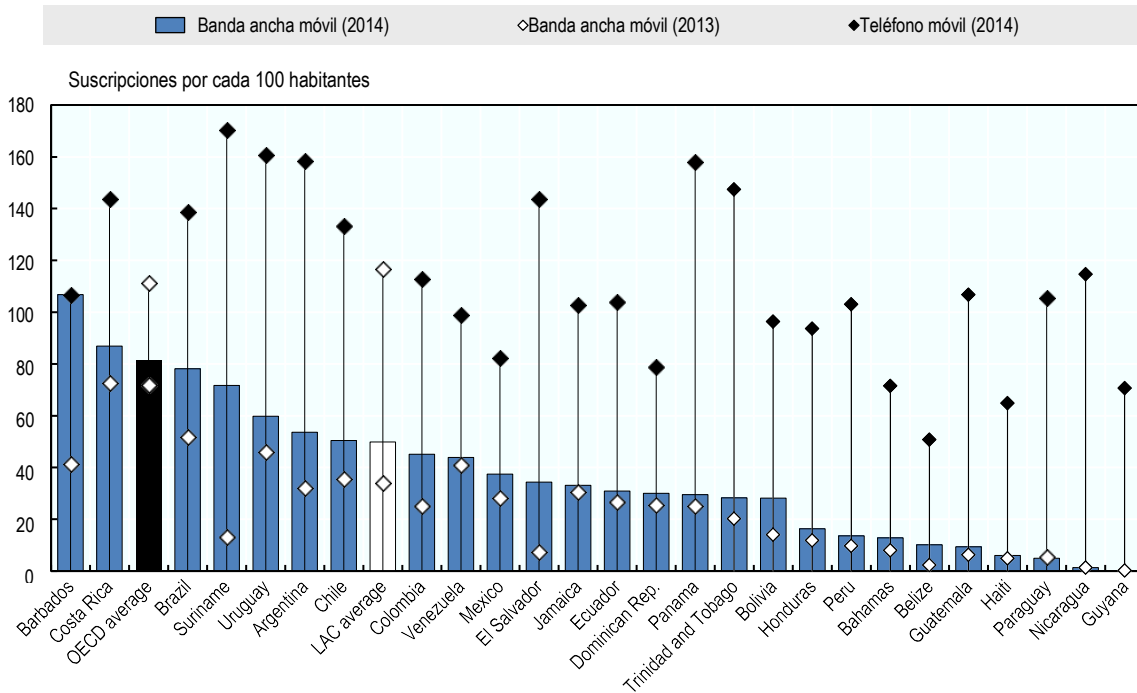


**Figura 2. Hogares con acceso a internet (fijo y móvil), 2008-2016**



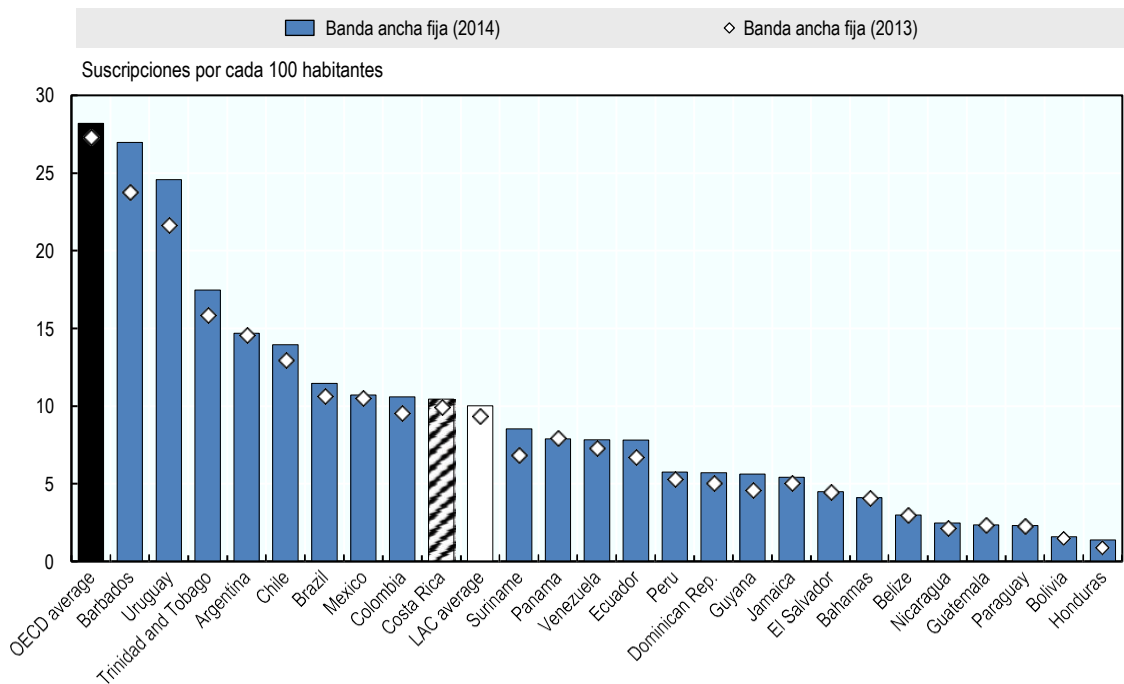
Fuente: Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica

**Figura 3. Penetración de telefonía y banda ancha móvil en ALC (2014)**



Fuente: OECD, 2016, Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit

**Figura 4. Penetración de banda ancha fija en ALC (2013-14)**



Fuente: OECD, 2016, Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit

### ***Marco jurídico***

La Ley N° 8642, Ley General de Telecomunicaciones (, en vigor desde 2008) regula el desarrollo de los mercados de comunicaciones en Costa Rica. Sus objetivos principales son promover la competencia efectiva y la convergencia de servicios, garantizar la transparencia y la neutralidad tecnológica, establecer las funciones de operadores y proveedores y reducir la brecha digital a través del acceso universal a los servicios.

La Ley N° 8660 de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, en vigor desde el 2008 y modificada por última vez en 2012, promueve los principios de neutralidad tecnológica, competencia efectiva, transparencia, optimización de recursos escasos y no discriminación.

### ***Responsabilidades y facultades***

El MICITT lidera el desarrollo de la banda ancha a través de la formulación de políticas públicas para desarrollar las telecomunicaciones y definir las metas y prioridades necesarias para implementar los objetivos del PNDT.

La SUTEL está a cargo de regular, supervisar, hacer cumplir y controlar el marco regulatorio de las telecomunicaciones. La SUTEL también es responsable de implementar los proyectos de acceso universal (incluido el desarrollo de banda ancha). Con este fin, la SUTEL administra el Fondo Nacional de Telecomunicaciones (FONATEL) y garantiza que los operadores de red y los proveedores de servicios de telecomunicaciones cumplan sus obligaciones de servicio y acceso universales. Costa Rica tiene un régimen mixto en materia de competencia: la Comisión para la Promoción de la Competencia (COPROCOM) del Ministerio de Economía, Industria y Comercio también aplica normas de competencia. La SUTEL es responsable de imponer sanciones a las prácticas anticompetitivas, pero requiere la opinión técnica de la COPROCOM. Ante conductas ilegales la SUTEL debe consultar a la COPROCOM tanto al comienzo del procedimiento como antes de tomar la decisión final.

## **2.2. Implementación**

### ***Competencia y liberalización continua***

Desde el inicio de la liberalización del mercado de las telecomunicaciones, Costa Rica ha fomentado la inversión privada en banda ancha. El PNDT 2015-2021 establece la política actual para el sector. La SUTEL promueve la competencia en Costa Rica y asegura que los operadores y proveedores puedan acceder al mercado de las telecomunicaciones en términos razonables y no discriminatorios. El Instituto Costarricense de Electricidad (ICE), que es el operador estatal de telecomunicaciones, todavía mantiene grandes cuotas de mercado (Tabla 1), pero otros operadores están activos en la prestación de servicios de banda ancha en Costa Rica.<sup>2</sup>

**Tabla 1. Cuota de mercado y tecnología utilizada por los operadores de banda ancha en Costa Rica, 2015**

	Empresa	Cuota de mercado	Tecnología/red
		(Suscriptores)	
<b>Principales proveedores de banda ancha fija a través de redes fijas</b>	Instituto Costarricense de Electricidad	45,4%	xDSL
	Millicom Cable Costa Rica, S.A.	23%	HFC Networks
	Televisora de Costa Rica, S.A.	16%	HFC Networks
	Telecable Económico, T.V.E, S.A.	9%	HFC Networks
<b>Proveedores de banda ancha fija a través de redes inalámbricas</b>	IBW Comunicaciones, S.A.	58%	WiMAX
	Instituto Costarricense de Electricidad	30%	WiMAX
	Radiográfica Costarricense, S.A.	5%	WiMAX
	Metro Wireless Solutions de Costa Rica MWS, S.A.	4%	Microwave links
<b>Proveedores de banda ancha móvil</b>	Instituto Costarricense de Electricidad	52%	2G/3G/4G
	Claro CR Telecomunicaciones, S.A.	26%	2G/3G/4G
	Telefónica de Costa Rica TC, S.A.	21%	2G/3G/4G

Fuente: Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica

### *Asignación y uso del espectro*

El MICITT está a cargo de la planificación, la atribución y la asignación del espectro de conformidad con el Artículo 10 de la Ley General de Telecomunicaciones, mientras que la SUTEL es responsable de las recomendaciones técnicas para la asignación y de la aplicación y el monitoreo de las regulaciones del espectro. El PNDT incluye la meta de asignar 890 MHz del espectro a sistemas internacionales de telecomunicaciones móviles para 2021, lo que promueve directamente la inversión privada al abrir el mercado de telecomunicaciones a los nuevos operadores en Costa Rica. El MICITT y la SUTEL están trabajando actualmente en una subasta de 70 MHz del espectro radioeléctrico, que se espera mejorará la calidad de los servicios y la experiencia del usuario final en las redes de IMT y abrirá la posibilidad de que nuevos operadores ofrezcan servicios de telefonía e internet móvil en el bandas de frecuencia de 1800 MHz y 1900/2100 MHz.

### *Iniciativas gubernamentales complementarias*

El Poder Ejecutivo de Costa Rica creó la Comisión de Coordinación para la Instalación o Ampliación de Infraestructura de Telecomunicaciones con el objetivo de acelerar el proceso de desarrollo de infraestructura, que a su vez elaboró un Plan de Acción de Infraestructura de Telecomunicaciones como una iniciativa pública destinada a mejorar la calidad de los servicios de telecomunicaciones en Costa Rica, incluido el acceso a internet.

### *Políticas del lado de la demanda*

El PNDT también establece objetivos y metas relacionadas con la creación de contenido digital y la alfabetización digital, así como esfuerzos para fortalecer los servicios en línea en áreas que incluyen la salud, la educación, el transporte y los servicios financieros, que se completarán en 2021. Se espera que estas nuevas ofertas de servicios aumenten la demanda de acceso de banda ancha.

### *Neutralidad tecnológica*

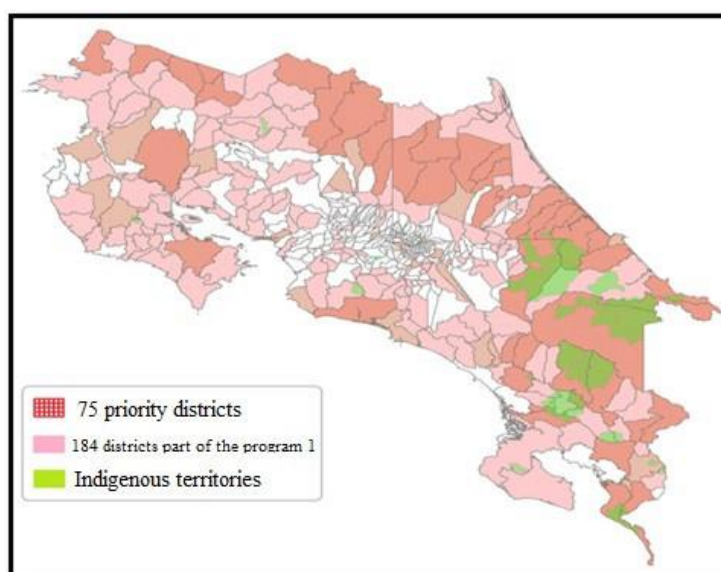
En Costa Rica las licencias de espectro son tecnológicamente neutrales. La Ley General de Telecomunicaciones les permite a los operadores de redes y proveedores de servicios de telecomunicaciones elegir cuáles tecnologías utilizar, siempre que garanticen la calidad del servicio y precios asequibles, según lo establece la ley.

### *Servicio universal*

Los servicios de acceso universal son financiados por el Fondo Nacional de Telecomunicaciones (FONATEL), al que todos los operadores y proveedores de servicios de telecomunicaciones contribuyen con tarifas que representan un porcentaje de su ingreso bruto total (entre 1.5% y 3%, definido anualmente por la SUTEL). En 2014, por ejemplo, el FONATEL recaudó aproximadamente USD 40.5 millones y desembolsó cerca de USD 8.3 millones. Los proyectos financiados por el FONATEL están destinados a reducir la brecha digital en las comunidades vulnerables en áreas como infraestructura, suministro de equipos y subsidios para las poblaciones en condiciones de pobreza.

En Costa Rica las áreas no rentables son definidas como áreas rurales, áreas alejadas y territorios indígenas en condición de vulnerabilidad social, económica y cultural. Algunas de estas áreas están incluidas en el programa denominado Comunidades Conectadas, que define las áreas prioritarias (Figura 5), los servicios que se ofrecerán y los requisitos de calidad pertinentes. El programa prevé una inversión pública de USD 168 millones dirigida a la modernización de la estructura de los servicios públicos, especialmente en las áreas de educación y salud. El programa abarcará 184 distritos ubicados a lo largo de todo el territorio nacional, que representan el 76% de la superficie del país y el 23% de la población de Costa Rica. El programa trabaja actualmente en parte de los 75 distritos prioritarios definidos como de alta prioridad (Figura 5, en rojo) y los 24 territorios indígenas en Costa Rica (Figura 5, en verde). La selección de los operadores que participan en el programa se define mediante licitaciones públicas. También se llevan a cabo procesos de consulta en las comunidades indígenas. Las obligaciones de los operadores también abarcan actividades de sensibilización, difusión y capacitación adaptadas a las zonas rurales durante un período de contrato de 5 años.

**Figura 5. Programa "Comunidades Conectadas": áreas prioritarias**



Fuente: Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica

El pilar de inclusión digital del PNDT tiene como objetivo reducir la brecha digital a través del acceso, el uso y la apropiación de tecnologías digitales para poblaciones en condiciones vulnerables, e incluye los siguientes programas:

1. *Comunidades conectadas*: con un presupuesto de USD 168 millones, el objetivo de este programa es proveer servicios fijos de voz e internet a instituciones públicas de educación y salud en 184 distritos de Costa Rica.
2. *Hogares conectados*: con un presupuesto de USD 100 millones, el objetivo de este programa es subsidiar el acceso a internet a 140 000 hogares en situaciones de pobreza y pobreza extrema (unas 507 000 personas), es decir, aproximadamente el 46% de los hogares costarricenses en situación de pobreza y pobreza extrema. Esto representa un aumento del 9% en la penetración de internet fija e implica que nueve de cada 100 hogares tendrían acceso a servicio de internet fijo.
3. *Centros públicos equipados*: con un presupuesto de USD 20 millones, el objetivo de este programa es suministrar computadoras a los centros públicos para ser utilizadas por personas con discapacidades, niños y niñas, jóvenes, personas adultas mayores, indígenas y mujeres jefas de hogar y microempresarias.
4. *Espacios públicos conectados*: con un presupuesto de USD 10 millones, el objetivo de este programa es conectar 240 puntos de acceso público con acceso gratuito a internet en todo el país.
5. *Red de banda ancha solidaria*: este programa está dirigido a centros de servicios públicos que tienen mayores necesidades de conectividad y su objetivo es mejorar la velocidad y la calidad de los servicios.
6. *Empoderamiento de la población en TIC*: este programa se centra en la educación y la seguridad en línea y su objetivo es mejorar la alfabetización digital.
7. *Programa Nacional de formación docente en TIC*: el objetivo de este programa es capacitar a los maestros en el uso de las TIC en el aula y, a su vez, enseñar a sus estudiantes el uso de las TIC.
8. *Plataforma tecnológica*: el objetivo de este programa es aumentar el uso de tecnologías digitales por parte de la niñez y las personas jóvenes en 317 escuelas del Ministerio de Educación Pública.

### *Una cultura de seguridad*

Las políticas de seguridad y privacidad digital en Costa Rica se detallan en otras secciones del presente informe.

## **2.3. Seguimiento y evaluación**

El seguimiento y la evaluación de la efectividad de la política de banda ancha está a cargo del MICITT. A los objetivos relacionados con banda ancha se les da seguimiento semestralmente, tal como se define en el PNDT. Además, Costa Rica tiene un Plan de Acción de Infraestructura de Telecomunicaciones; la Comisión de Infraestructura, conformada por instituciones públicas y dirigida por el MICITT, les da seguimiento a sus acciones mensualmente.

La SUTEL presenta semestralmente a la Contraloría General y el MICITT los datos relacionados con la cobertura de los servicios, los aspectos financieros, el desempeño y el estado de ejecución de los proyectos financiados por el FONATEL. Esta información también se envía al congreso costarricense una vez al año. La SUTEL publica anualmente un "Informe de estadísticas del sector de telecomunicaciones" que mide la evolución de las telecomunicaciones en Costa Rica.

La información incluida en estos informes se utiliza para desarrollar y ajustar las iniciativas gubernamentales. Con base en la evaluación y el seguimiento de la política de banda ancha se actualizan las metas y los objetivos relacionados con la política de banda ancha.

## 2.4. Evaluación

### ***Recomendación del Consejo relativa al desarrollo de la banda ancha [OECD/LEGAL/0322]***

El marco establecido para el desarrollo de la banda ancha en Costa Rica refleja los principios contenidos en la Recomendación sobre banda ancha, incluidos los principios de competencia efectiva y liberalización continua, neutralidad tecnológica, transparencia, enfoques basados en la oferta y la demanda, la no discriminación y la objetividad de los criterios, las condiciones y los procedimientos de regulación.

En los últimos años la infraestructura de banda ancha en Costa Rica ha mejorado significativamente como resultado de las políticas de liberalización y desarrollo de banda ancha establecidas en la Estrategia Nacional de Banda Ancha y luego en el PNDT. La penetración de la banda ancha móvil en Costa Rica, con un 86.9% en 2014 y 90% en 2015, es alta cuando se compara con los promedios de América Latina y el Caribe (ALC) y la OCDE, mientras que la penetración de la banda ancha fija fue mayor que la media en ALC pero considerablemente más baja en la medida de la OCDE. El marco de Costa Rica fomenta la inversión y la competencia en infraestructura y servicios de banda ancha. El pilar de inclusión digital del PNDT incluye iniciativas tanto de oferta como de demanda para ampliar los servicios y oportunidades de banda ancha en áreas desatendidas y en hogares vulnerables o en situación de pobreza.

Según el PNDT, el objetivo del gobierno es dar acceso de banda ancha según los estándares de la OCDE para la población costarricense en el 2021. El número de suscriptores de internet (fija y móvil) y el número de usuarios de internet (fija y móvil) han aumentado drásticamente entre 2008 y 2016. Los proveedores continúan instalando redes de telefonía móvil en todo el país, de conformidad con los planes de implementación establecidos en los contratos de concesión. Además, el gobierno está desarrollando proyectos de acceso y servicio universales en áreas donde, para los proveedores, no es económicamente viable implementar infraestructura.

### 3. ITINERANCIA MÓVIL INTERNACIONAL

#### 3.1. Políticas

El objetivo de la política de itinerancia de Costa Rica es proteger los derechos de los usuarios finales de los servicios de telecomunicaciones y disminuir la cantidad de reclamaciones sobre itinerancia móvil internacional (IMI) presentadas ante la SUTEL.

##### *Marco regulatorio*

La itinerancia internacional, como parte de los servicios de telecomunicaciones, está sujeta a la Ley N° 8642, Ley General de Telecomunicaciones (LGT), que promueve la competencia efectiva basada en el análisis de los mercados relevantes y la regulación *ex ante*. Los usuarios finales de los servicios de itinerancia internacional también están protegidos por las obligaciones y los requisitos de transparencia de los operadores, incluida la obligación de proporcionar a sus usuarios información de facturación y permitirles limitar la cantidad mensual gastada en servicios de IMI.

Con base en la recomendación de la Unión Internacional de Telecomunicaciones (UIT), ITU- T D.98, "Cobro en los servicios de itinerancia móvil internacional", la SUTEL emitió una resolución en 2014 sobre "Disposiciones regulatorias aplicables a los servicios de Roaming Internacional" (Resolución N° RCS-041-2014) que contiene disposiciones reglamentarias generales aplicables a los servicios de itinerancia internacional:

- a. Facilitar información sobre las condiciones de uso y las tarifas en el momento de suscribir el contrato de adhesión.
- b. Notificar a los usuarios que usen itinerancia a través de un mensaje de texto SMS gratuito que contenga: *i*) un mensaje de bienvenida; *ii*) las tarifas de itinerancia internacional aplicables al realizar y recibir llamadas de voz; *iii*) las tarifas de itinerancia internacional aplicables al enviar y recibir mensajes SMS; *iv*) las tarifas de itinerancia internacional aplicables por el acceso a internet; *v*) una advertencia sobre el riesgo de las descargas automáticas en itinerancia internacional; *vi*) un enlace a sitios web donde se publican las tarifas; y *vii*) un número telefónico gratuito para realizar consultas y recibir asistencia.
- c. El número de teléfono de soporte, ya sea local o internacional, debe ser gratuito.
- d. Se debe proporcionar información sobre cómo evitar las tarifas de itinerancia internacional en las regiones fronterizas.
- e. Las tarifas publicadas en los sitios web de los respectivos operadores deben mantenerse actualizadas y se les debe notificar a los usuarios acerca de cualquier cambio de precios.

Además, la resolución establece que los operadores o proveedores de servicios que prestan servicios de itinerancia internacional deben: *a*) proporcionar ejemplos sobre el uso de itinerancia internacional al momento de firmar el contrato; *b*) informar a los usuarios al momento de firmar el contrato acerca de los costos financieros de las conexiones de itinerancia internacional y las descargas automáticas de datos; *c*) informar a los usuarios que tienen activado el servicio de itinerancia internacional de los costos financieros asociados con estas conexiones y descargas automáticas a través de mensajes de texto al menos cada 3 meses; *d*) informar a los usuarios también por correo electrónico, aunque los correos electrónicos no sustituyen la necesidad de enviar un SMS; *e*) proporcionarles a los usuarios del servicio de itinerancia internacional un mecanismo gratuito para que obtengan información sobre el consumo acumulado, accesible a través de SMS y 24/7; *f*) asegurarse de que cada período de facturación no exceda un límite financiero específico; *g*) establecer un límite financiero de USD 200 si el usuario no establece un límite diferente; *h*) notificar por SMS cuando el usuario haya alcanzado el 80% de su límite financiero; e *i*) cuando

exceda el límite, se le debe notificar al usuario el procedimiento para continuar la prestación de los servicios de itinerancia internacional, así como las tarifas por cada unidad adicional que consuma.

### ***Responsabilidades y facultades***

La autoridad reguladora de las telecomunicaciones (SUTEL) supervisa las reglas de los servicios de itinerancia internacional. La SUTEL supervisa y controla la calidad del servicio; protege los derechos del usuario final; y procesa, investiga y resuelve las reclamaciones derivadas de la violación de sus derechos (de conformidad con los artículos 41 y 42, Capítulo II, Título II de la Ley General de Telecomunicaciones, de conformidad con el Reglamento interno de organización y funciones de la Autoridad Reguladora de los Servicios Públicos).

El MICITT también desempeña una función importante, especialmente en la formulación de políticas y la coordinación internacional.

## **3.2. Implementación y aplicación**

Los operadores presentes en América Central y otros países han estimulado el mercado minorista de servicios de itinerancia internacional. Los servicios ofrecidos varían según el operador; sin embargo, la competencia actual en el mercado ha traído beneficios a los usuarios de servicios de IMI. Claro aplica tarifas y cuotas locales a sus clientes prepago que viajan a Guatemala, El Salvador, Honduras, Nicaragua y Panamá. Movistar Costa Rica cobra a sus clientes pospago tarifas locales cuando viajan a Guatemala, El Salvador, México, Honduras y Panamá y les permite a sus clientes pospago usar su paquete de datos locales cuando viajan a los Estados Unidos, Canadá, Argentina, Brasil, Chile, Colombia, Ecuador, Perú, Uruguay y la República Bolivariana de Venezuela por USD 5 por día.

## **3.3. Seguimiento y evaluación**

La SUTEL supervisa la efectividad de las políticas de itinerancia móvil internacional mediante el seguimiento de la evolución de las reclamaciones pertinentes. El número de reclamaciones recibidas entre 2012 y 2013 aumentó drásticamente en un 233%. Por este motivo, entre otros, la SUTEL emitió la Resolución N° RCS-041-2014 en 2014 mencionada anteriormente. Las reclamaciones por IMI han disminuido desde 2014, con 24 reclamaciones en 2015 y solo 4 en el primer semestre de 2016.

## **3.4. Evaluación**

### ***Recomendación del Consejo relativa a los servicios de itinerancia móvil internacional [OCDE/LEGAL/0388]***

Los objetivos principales de la política de itinerancia móvil internacional de Costa Rica son reducir el daño cometido a los usuarios finales y disminuir la cantidad de reclamaciones sobre itinerancia internacional que recibe la SUTEL. La Resolución N° RCS-041-2014 aporta una serie de medidas para cumplir estos objetivos. Costa Rica participa en iniciativas de organizaciones regionales como COMTELCA y REGULATEL dirigidas a reducir los precios de la itinerancia móvil internacional, pero la dinámica del mercado en Costa Rica ya conduce a los operadores a ofrecer planes competitivos de itinerancia móvil internacional. Además, las reclamaciones relacionadas con itinerancia móvil internacional se redujeron drásticamente después de publicada la resolución de la SUTEL.

## 4. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

### 4.1. Políticas

El Viceministerio de Telecomunicaciones del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), con el apoyo de la Organización de los Estados Americanos (OEA), desarrolló la Estrategia Nacional de Ciberseguridad de Costa Rica adoptada en octubre de 2017. La estrategia está alineada con los objetivos principales de la visión de desarrollo nacional de largo plazo "Costa Rica 2030"; con el Plan Nacional de Desarrollo 2015-2018 "Alberto Cañas Escalante" (PND), que considera la ciberseguridad en los servicios públicos en línea como parte del programa de gobierno electrónico; y con el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 (PNDT), que tiene como objetivo: "Transformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones; de forma segura, responsable y productiva."

En los procesos de consulta de la Estrategia Nacional de Ciberseguridad han participado varias instituciones estatales, entidades privadas, la academia, la sociedad civil y el regulador de telecomunicaciones. Desde marzo de 2015 el Viceministerio de Telecomunicaciones ha organizado, a través de su Departamento de Gobierno Electrónico y con el apoyo técnico de la OEA, tres mesas redondas, cuatro talleres sectoriales y dos consultas en línea. Participaron cerca de 120 partes interesadas de los sectores público y privado, con una representación notable del sector de las telecomunicaciones y de infraestructura crítica, así como de la sociedad civil.

La estrategia de seguridad cibernética se centra en la economía y en un amplio desarrollo de capacidades. Su objetivo es garantizar los niveles de ciberseguridad y resiliencia cibernética adecuados para apoyar la economía digital del país y lograr prosperidad económica y social mediante el desarrollo de recursos humanos y tecnológicos capaces de prevenir y mitigar los riesgos del uso de las TIC. Articula el contexto económico y social de Costa Rica, en particular la economía nacional, donde las exportaciones de TIC representaron el 50% del comercio exterior en 2013, y los objetivos clave de políticas públicas de mejorar la conectividad y desarrollar el gobierno electrónico en Costa Rica. El enfoque de desarrollo e implementación de la estrategia implica basarse en los procesos y las instituciones existentes de manera flexible.

La estrategia proporciona *i)* contexto nacional (ver arriba); *ii)* cuatro principios rectores: prioridad a las personas y respeto a los derechos humanos y la privacidad, garantizar la responsabilidad compartida y la coordinación entre múltiples partes interesadas, alentar el uso individual responsable de las TIC, y promover la cooperación internacional; *iii)* el objetivo general de "*[d]esarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país*"; *iv)* objetivos específicos; *v)* ocho amplias líneas de acción (ver más adelante); y *vi)* los actores principales.

La estrategia establece las siguientes líneas de acción:

1. **coordinación nacional**, que incluye el intercambio de información respaldado por acuerdos de confidencialidad y la colaboración de las partes interesadas de los sectores público y privado, y planes para la creación de una red de intercambio de información entre las entidades gubernamentales.

2. **Campañas de concienciación** dirigidas a: *i)* el público en general; *ii)* funcionarios públicos, respecto de las mejores prácticas para proteger y asegurar el acceso a los sistemas de información y proteger los datos confidenciales y personales; *iii)* responsables de las decisiones; *iv)* gobiernos locales.
3. **Desarrollo de habilidades en ciberseguridad:** *i)* desarrollar planes de estudio académicos en ciberseguridad en asociación con instituciones educativas – especialmente escuelas científicas y otras que tengan laboratorios de informática– y organismos de acreditación<sup>3</sup>; *ii)* promover el desarrollo de profesionales en seguridad cibernética en Costa Rica; *iii)* establecer alianzas y proyectos de investigación con universidades públicas y privadas sobre amenazas emergentes; *iv)* PYMES.
4. **Fortalecimiento del marco jurídico** en ciberseguridad y ciberdelincuencia a través de: *i)* para los delitos cibernéticos, la creación de un comité especializado que revise la legislación y la normativa existente y garantice la idoneidad de las herramientas procesales en materia de delincuencia cibernética; *ii)* el desarrollo de las capacidades de las partes interesadas en el sistema de justicia penal, p. ej. a través de la Escuela Judicial, para capacitar a los actores del poder judicial, incluidos los jueces, sobre temas como la evidencia en los delitos cibernéticos; *iii)* intercambio de información facilitado por disposiciones de confidencialidad.
5. **Protección de infraestructuras críticas de información (ICI)**, especialmente la seguridad de los sistemas y redes de información con apoyo de las entidades públicas, a través de: *i)* la identificación de la infraestructuras críticas; y *ii)* la creación de una comisión, compuesta por un representante y un suplente de cada una de las instituciones públicas y las entidades privadas identificadas, que se encargue de desarrollar una política de protección de ICI que garantice la operatividad y la estabilidad de estos servicios.
6. **Gestión de riesgos:** la estrategia planea utilizar marcos de gestión de riesgos y tomar en consideración estándares internacionales, incluido el modelo de gestión de riesgos del Software Engineering Institution (SEI), el marco de gestión de riesgos de FISMA y la serie de normas ISO/IEC INTE 27000, entre otros modelos.
7. **Cooperación y compromiso internacional:** la estrategia planea que Costa Rica desarrolle asistencia mutua en materia penal, técnica y educativa, así como desarrollar medidas internacionales de seguridad para abordar asuntos de ciberseguridad. Costa Rica firmó una carta de entendimiento con la Agencia Coreana de Seguridad de Internet (KISA) y es miembro de la Alianza de Ciberseguridad para el Progreso Mutuo (CAMP).
8. **Seguimiento y evaluación:** los planes estratégicos prevén que las partes interesadas, incluidos los ministerios públicos y los reguladores sectoriales, presenten informes periódicos al Coordinador Nacional de Ciberseguridad, quien evaluará el progreso en consulta con CSIRT; también incluye plantear recomendaciones e informar anualmente al Presidente de la República y al Consejo de Ministros.

### ***Marco jurídico y regulatorio***

El marco jurídico y regulatorio vigente en materia de seguridad digital incluye:

- **Protección de datos:** La Ley N° 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales creó la Agencia de Protección de Datos de los Habitantes (PRODHAB) en 2011 para garantizar el cumplimiento de las normas de protección de datos. El Reglamento sobre medidas para proteger la privacidad de las comunicaciones también incluye disposiciones para la

protección de datos, conforme al artículo 42 de la Ley N° 8642, Ley General de Telecomunicaciones.

- **Cibercrimen:** la Unidad de Delitos Informáticos del Organismo de Investigación Judicial (OIJ) fue creada en 1997 para investigar los delitos cibernéticos y otros casos en los que se utilicen computadoras en un delito o como evidencia, utilizando técnicas forenses informáticas. La Ley N° 9048 de 2012 sobre delitos informáticos y las modificaciones del Código Penal en materia de delitos informáticos y conexos (Sección VIII) establecieron un sistema penal más completo, que abarca los nuevos delitos cometidos por medios tecnológicos. En mayo de 2017, Costa Rica dio su aprobación final para adherirse a la Convención sobre Ciberdelincuencia (conocida como la “Convención de Budapest”).
- **Identificación:** La Ley N° 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, de 2005 asocia la identidad de una persona física o jurídica con un mensaje o documento electrónico para garantizar así la autoría y la integridad y es aplicable a muchos tipos de transacciones públicas o privadas y actos jurídicos.
- **Respuesta a incidentes de seguridad informática:** El Decreto Ejecutivo (N° 37052-MICITT) creó el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR) en 2012 con el mandato de actuar como un organismo de consulta sobre seguridad de las TIC y el objetivo de ayudar al sector público a desarrollar planes de contingencia de seguridad de las TIC y promover proyectos de investigación y capacitación en seguridad de las TIC.
- **Protección infantil:** la Ley N° 8934 de Protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos, de 2011.

### *Responsabilidades y facultades*

El MICITT lidera el área de ciberseguridad y establece los objetivos relacionados con la ciberseguridad en el Plan Nacional de Desarrollo de las Telecomunicaciones (PNDDT). La Estrategia de Ciberseguridad encarga al MICITT la responsabilidad de articular todas las acciones entre entidades públicas y privadas que define la estrategia, así como de promover la participación de todas las partes interesadas, incluidos CSIRT-CR, PRODHAB, la Unidad de Delitos Informáticos del OIJ y otros actores relevantes como, por ejemplo, la SUTEL, los ISP y los administradores de infraestructura crítica.

La función del CSIRT-CR es coordinar la ciberseguridad dentro de las ramas gubernamentales, las instituciones autónomas, las empresas y los bancos estatales, incluidos los marcos de gestión de riesgos, con los objetivos de: promover y supervisar los planes de contingencia relacionados con la seguridad de las TIC en el sector público; promover proyectos de investigación y capacitación sobre seguridad de las TIC; coordinar con los operadores de ICI y otros activos críticos o servicios esenciales para garantizar la ejecución de planes de continuidad; y cooperar y coordinar con sus pares internacionales. El Decreto Ejecutivo pertinente prevé que el CSIRT-CR tendrá "sede en las instalaciones del Ministerio de Ciencia y Tecnología, con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado". El CSIRT-CR entró en funcionamiento en octubre de 2017, compuesto por cuatro expertos. Se están realizando esfuerzos para asegurar y aumentar sus recursos en el transcurso de 2018 gracias a acuerdos entre el MICITT y otros ministerios e instituciones gubernamentales.”

La Unidad de Delitos Informáticos del OIJ fue creada en 1997 para investigar los delitos cibernéticos y otros casos en los que se utilicen computadoras en un delito o como evidencia, utilizando técnicas forenses informáticas para recopilar, conservar y analizar pruebas en dispositivos de procesamiento y almacenamiento de datos; por ejemplo, computadoras, discos duros, llaves USB o teléfonos celulares. Los principales delitos que persiguen son el fraude informático, la violación de comunicaciones electrónicas, la

alteración de datos y el sabotaje de computadoras y la producción, posesión y distribución de pornografía infantil.

Una "Comisión Nacional de Seguridad en Línea", un órgano interinstitucional creado en 2004, trabaja en el desarrollo de proyectos de seguridad relacionados con la protección infantil.

La Agencia de Protección de Datos de los Habitantes (PRODHAB) garantiza el cumplimiento de las normas de protección de datos, ayuda a redactar leyes para implementar normas de protección de datos personales y emite directrices para que las instituciones públicas implementen procedimientos adecuados para el manejo de los datos personales.

Se considera que todas las partes interesadas desempeñan una función en el desarrollo y la implementación de políticas relacionadas con la gestión de riesgos de ciberseguridad. La entidad operativa que garantizará la implementación eficaz de la estrategia es la Dirección de Gobernanza Digital, que ayudará en la ejecución, coordinación y seguimiento interinstitucional e intersectorial mediante el establecimiento de canales de comunicación, trabajo conjunto y espacios de diálogo con todas las partes interesadas.

La Estrategia también destaca la necesidad de que participen:

- Los gobiernos locales, con programas digitales que orienten sus acciones de ciberseguridad.
- Actores del poder judicial, que deben proteger la información sensible o confidencial que se intercambia durante consultas y solicitudes de información (p. ej., en el sitio web de servicios judiciales) o que sirve de evidencia electrónica; y cabe destacar que el poder judicial coordina con el gobierno la estrategia de seguridad cibernética, aunque es independiente del gobierno y tiene su propia estrategia digital.
- Las empresas de telecomunicaciones, a través de directrices y mecanismos gubernamentales que les ayuden a coordinar, compartir información en caso de ataques cibernéticos y documentar sistemáticamente los incidentes. La estrategia hace referencia a una encuesta realizada por la SUTEL a 17 compañías de telecomunicaciones en 2015 que identificó la necesidad de contar con medidas para coordinar y compartir información entre los distintos actores. En ella, un tercio de los encuestados dijeron haber detectado amenazas potenciales o haber sido atacados en el año anterior, el 100% dijo haber identificado su infraestructura esencial y el 83% dijo tener procedimientos para controlar y monitorear los cambios que experimente la infraestructura).
- Empresas del sector financiero, a través del desarrollo de mejores prácticas y requisitos mínimos para la seguridad de la información en el sector financiero, en coordinación con el ente regulador.

### ***Cooperación internacional***

Las políticas y prácticas de Costa Rica para combatir el fraude transfronterizo se detallan en la Sección 4 de la evaluación sobre Política del Consumidor en Costa Rica. En particular, los organismos judiciales y civiles de aplicación de la ley en Costa Rica cooperan en las investigaciones penales transfronterizas con otros organismos a través de INTERPOL, la organización policial internacional. Se prevé que la reciente ratificación de Costa Rica de la Convención sobre Ciberdelincuencia del Consejo de Europa (también conocida como la "Convención de Budapest") proporcionará un marco útil para el aceleramiento del intercambio de información sobre ciberdelincuencia y los procedimientos legales y los acuerdos institucionales necesarios para que las investigaciones y el procesamiento judicial sean eficaces y, al mismo tiempo, protejan el derecho a la privacidad de las personas.

## 4.2. Seguimiento y evaluación

La ciberseguridad en los servicios públicos ya forma parte del Programa de Gobierno Electrónico establecido por el Plan Nacional de Desarrollo 2015-2018 "Alberto Cañas Escalante" (PND), que estableció la meta del 20% de los ministerios (nueve ministerios) que hayan implementado un Protocolo de Seguridad Cibernética en 2017 y del 50% en 2018.

La Estrategia Nacional de Ciberseguridad incluye el diseño de un modelo de seguimiento y evaluación que permitirá ajustar las acciones para que reflejen los cambios en las condiciones. El MICITT planea evaluar y revisar la Estrategia de Ciberseguridad cada tres años, en colaboración con la OEA.

## 4.3. Valoración y recomendaciones

### ***Recomendación del Consejo sobre gestión de riesgos de seguridad digital para fomentar la prosperidad económica y social [OCDE/LEGAL/0415]***

En la sesión del CDEP del 17 de mayo de 2017, Costa Rica reconoció la oportunidad de alinear su Estrategia Nacional de Seguridad Digital y la Recomendación del Consejo sobre gestión de riesgos de seguridad digital para fomentar la prosperidad económica y social. La Estrategia Nacional de Seguridad Digital de Costa Rica sienta las bases y coordina el proceso de planificación de la seguridad digital y está alineada con la visión a largo plazo de Costa Rica para el desarrollo nacional "Costa Rica 2030", el PND 2015-2018 y el PNDDT 2015-2021. Este último tiene como objetivo "[t]ransformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones; de forma segura, responsable y productiva." También considera la ciberseguridad como un asunto esencial.

Los principios de la Recomendación del Consejo sobre gestión de riesgos de seguridad digital para fomentar la prosperidad económica y social se reflejan en la Estrategia Nacional de Ciberseguridad de Costa Rica. El propósito general de la política es facilitar el crecimiento de la economía digital del país y la consecuente prosperidad económica y social. Sus objetivos incluyen promover medidas de educación, prevención y mitigación de los riesgos del uso de las TIC, a fin de lograr un entorno más seguro y confiable para todos los habitantes del país. La Estrategia provee principios rectores y objetivos estratégicos para abordar los riesgos de seguridad digital y combatir los delitos cibernéticos, lo cual incluye la protección de los derechos humanos, el empoderamiento de las partes interesadas, la gestión del riesgo y la cooperación internacional.

Costa Rica está desarrollando un enfoque nacional flexible para los riesgos de seguridad digital bajo los marcos y procesos nacionales vigentes. Como parte de la estrategia de gobierno electrónico de Costa Rica, el MICITT es responsable de desarrollar y promover la estrategia de seguridad cibernética y de coordinar la implementación de un protocolo de seguridad cibernética en las instituciones públicas. La estrategia planea que las instituciones públicas mantengan la propiedad de sus protocolos de seguridad digital con la asistencia del MICITT, lo que ayudará a garantizar que las medidas de seguridad digital se diseñen de manera adecuada y acorde con los riesgos que enfrentan. Costa Rica parece estar abordando la estrategia nacional de manera constructiva y con objetivos útiles, como comenzar con protocolos de seguridad digital y planes de continuidad en el sector público. La estrategia de Costa Rica garantizará el liderazgo al más alto nivel y la participación de todos los sectores, más allá del énfasis en las telecomunicaciones.

### ***Recomendaciones***

- Continuar garantizando el conocimiento y la comprensión de la gestión de riesgos de seguridad digital por parte de las personas encargadas de adoptar decisiones y las responsables de la formulación de políticas.
- Asegurar la implementación efectiva de la Estrategia Nacional de Seguridad Digital de Costa Rica mediante la ejecución, coordinación y seguimiento entre los distintos órganos y de manera intersectorial.
- Asegurar un presupuesto explícito y asignaciones de personal que permitan que el CSIRT-CR desarrolle y amplíe la escala de sus operaciones.

## 5. PROTECCIÓN DE LA INFRAESTRUCTURA DE INFORMACIÓN CRÍTICA

### 5.1. Políticas

La estrategia de seguridad cibernética de Costa Rica (véase la Sección 4) incluye una sección sobre la protección de la infraestructura de información crítica (ICI). Subraya la prioridad de identificar las infraestructuras críticas en los sectores público y privado y planea la creación de una Comisión compuesta por representantes de cada una de las instituciones públicas y las entidades privadas identificadas como ICI para desarrollar políticas que garanticen la operación y protección continuas de estos servicios.

La Estrategia destaca el papel clave de los propietarios y operadores de las ICI en el uso de marcos específicos para gestionar los riesgos de seguridad; por ejemplo, en la adquisición de bienes y servicios de TIC<sup>4</sup>; en la creación de políticas de control y acceso; y en el abordaje de posibles vulnerabilidades. También identifica la necesidad de que los reguladores en los sectores clasificados como infraestructura crítica asuman un papel más destacado y comiencen a definir y dictar directrices claras en materia de ciberseguridad, en la forma de reglamentos, normas y mejores prácticas. La estrategia dice que tomará en consideración estándares internacionales como la ISO 27001 y la ISO 27002, NERC CIP-002-3 a CIP-009-3, la publicación especial 800-82 del NIST y el Marco de mejora de la ciberseguridad de las infraestructuras críticas. Para mitigar las violaciones de la seguridad también identifica la necesidad de una mayor cooperación entre los operadores de infraestructuras críticas; por ejemplo, las centrales eléctricas y las redes de suministro, los sistemas financieros y fiscales, la atención médica, servicios de agua y transporte, los proveedores de servicios de TIC, los proveedores de sistemas y el estado.

#### *Marco jurídico y regulatorio*

Actualmente Costa Rica no cuenta con disposiciones legales específicamente dedicadas a la protección de la ICI. Las leyes detalladas en la Sección 4 sobre la creación del CSIRT-CR y sobre la ciberdelincuencia son pertinentes para la protección de las ICI, al igual que la nueva "Ley de delitos informáticos" (Ley N° 9048) y el Código Penal actualizado (Sección VIII, Título VII) en materia de delitos informáticos y conexos.

#### *Responsabilidades y facultades*

El MICITT desarrollará la política de ICI, para lo cual tendrá la responsabilidad de coordinar con las partes interesadas en la medida de sus capacidades y recursos. Una vez que se identifiquen las ICI, la estrategia prevé la creación de una Comisión –compuesta por el MICITT y por representantes de las instituciones y empresas que administran la infraestructura crítica– encargada de desarrollar las políticas que garanticen la operación continua y la estabilidad de estos servicios.

La función del CSIRT-CR es coordinar la ciberseguridad entre los actores públicos y privados para promover y supervisar los planes de contingencia relacionados con la seguridad de las TIC en el sector público; promover proyectos de investigación y capacitación sobre seguridad de las TIC; coordinar con los operadores de ICI y otros activos críticos o servicios esenciales para garantizar la ejecución de planes de continuidad; y cooperar y coordinar con sus pares internacionales. El MICITT ha suministrado fondos y personal adicional al CSIRT-CR, que ahora cuenta con cuatro expertos. Se está considerando la financiación del CSIRT en el presupuesto de 2018.

Los propietarios y operadores de ICI son responsables de implementar las políticas de ICI.

## 5.2. Valoración y recomendaciones

### ***Recomendación del Consejo sobre la protección de las infraestructuras críticas de información [OCDE/LEGAL/0361]***

La estrategia de seguridad cibernética recientemente adoptada reconoce la necesidad de proteger las infraestructuras críticas de información (ICI). Una ley de 2015 creó el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR) con el objetivo de desarrollar la capacidad institucional para proteger las ICI en Costa Rica. Las modificaciones del Código Penal penalizan los delitos informáticos como el sabotaje y el espionaje y las identidades digitales, y los datos personales y la privacidad de las personas en línea están protegidos por la Ley N° 8968 sobre datos personales.

### ***Recomendaciones***

- Asegurar que exista un presupuesto explícito y las asignaciones de personal que permitan que el CSIRT-CR desarrolle y amplíe la escala de sus operaciones (esta recomendación también se incluye en la sección de Gestión de riesgos de seguridad digital).

## 6. CRIPTOGRAFÍA

### 6.1. Políticas

Actualmente Costa Rica no tiene una política de criptografía y no tiene planificado desarrollar una. La criptografía se utiliza principalmente en los sectores financiero y público, donde existen pocas políticas y los controles asociados. Los diferentes productos y servicios que requieren el uso de métodos criptográficos especifican sus propias políticas en términos de riesgo y selección de algoritmos, protección del material criptográfico y responsabilidad de los usuarios y la administración. Por ejemplo, el Sistema Nacional de Certificación Digital (SNCD) del MICITT tiene una Política de Certificados (CP) para la jerarquía nacional de certificadores registrados que reúne las reglas sobre el uso de criptografía en certificados y firmas digitales (2013).

#### *Marco jurídico y regulatorio*

La Ley N° 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, de 2005, regula las firmas digitales, que son uno de los principales usos de la criptografía en Costa Rica. Esta Ley le otorga a la firma digital el mismo valor y eficacia probatoria que sus equivalentes firmadas en manuscrito (artículos 8, 9 y 10). Además, la Ley estipula que los certificados digitales pueden garantizar, confirmar o validar técnicamente la integridad, autenticidad y no alteración de documentos en general (artículo 11) y faculta al Estado, a instituciones públicas y a empresas públicas y privadas, las personas jurídicas y las personas físicas a establecer los mecanismos de certificación o validación que convengan a sus intereses (artículo 12). Para ello, pueden utilizar mecanismos de certificación o validación que ofrezcan seguridad óptima: máquina a máquina, persona a persona, programa a programa y sus interrelaciones, o sistemas de llave pública y llave privada, firma digital y otros mecanismos digitales. En este sentido, esta Ley contribuye a promover la confianza y la elección de los métodos criptográficos.

El Decreto Ejecutivo N° 33018, Reglamento de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (2006), establece que el contenido de los certificados digitales, las condiciones de su emisión, la suspensión, la revocación y la caducidad deben cumplir con la Norma INTE/ISO 21188: “Infraestructura de llave pública para servicios financieros. Estructura de prácticas y políticas”, en su versión vigente, y con las políticas emitidas por la Dirección de Certificadores de Firma Digital (Artículo 5).<sup>5</sup> En relación con los certificadores, el Reglamento estipula que, para obtener la condición de certificador registrado, el solicitante debe poseer idoneidad técnica y administrativa, que serán valoradas por el Ente Costarricense de Acreditación, de conformidad con los lineamientos técnicos establecidos en las Normas INTE-ISO/IEC 17021:2007, Evaluación de la conformidad — Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión (artículo 11). Esta ley promueve la confianza en la criptografía y en las normas que la regulan.

La Ley N° 8968 de Protección de la persona frente al tratamiento de sus datos personales (2011) tiene como objetivo garantizar a cualquier persona el respeto de sus derechos fundamentales, en particular derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad. También procura garantizar la defensa de la libertad y la igualdad con respecto al procesamiento de datos personales. Esta ley y sus reglamentos estipulan medidas legales y técnicas para garantizar la transferencia de datos personales de modo que se respeten los derechos de los ciudadanos sin afectar el comercio internacional. La ley protege los datos personales y la privacidad.

La Ley N° 8642, Ley General de Telecomunicaciones de 2008, dispone que los operadores de redes públicas y los proveedores de servicios de telecomunicaciones disponibles al público deben garantizar el secreto de las comunicaciones y proteger la intimidad y los datos personales de los suscriptores y usuarios finales (artículo 42). Los operadores y proveedores deben tomar las medidas técnicas y administrativas adecuadas para garantizar la seguridad de las redes y los servicios y deben informar a la SUTEL y a los usuarios finales al percatarse de la existencia de riesgo para la seguridad de la red. Los operadores y proveedores deben asegurarse de que las comunicaciones y los datos de tráfico asociados con ellas no sean escuchadas, grabadas, almacenadas, modificadas o controladas por terceros sin consentimiento, excepto con la autorización judicial correspondiente.

La adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos, establece penas de prisión: *i*) a la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos (de seis meses a dos años); *ii*) a las personas a cargo de soportes electrónicos, informáticos, magnéticos y telemáticos que lleven a cabo las acciones descritas en el inciso anterior (uno a tres años de prisión); *iii*) por alterar datos sin autorización y por sabotaje informático (de uno a cuatro años de prisión); *iv*) si el comportamiento indicado impide o inhabilita la operación de un programa informático, base de datos o sistema informático (tres a seis años de prisión); *v*) se incrementa si el programa informático, la base de datos o el sistema informático contiene datos públicos (hasta ocho años).

El proceso judicial en Costa Rica requiere del debido proceso para acceder a información de carácter privado, lo que también respalda el acceso legal y la responsabilidad.

## 6.2. Implementación

Todas las personas y entidades en Costa Rica son libres de desarrollar, elegir y usar cualquier método y producto criptográfico y el gobierno no controla las importaciones o exportaciones de estos productos. Los sistemas informáticos de contratación pública utilizan firmas digitales como mecanismo de autenticación. El gobierno no ha establecido un estándar de criptografía, a pesar de que las instituciones pueden usar cualquiera.

## 6.3. Evaluación

### ***Recomendación del Consejo relativa a directrices sobre política de criptografía [OCDE/LEGAL/0289]***

Costa Rica no tiene una política centralizada de criptografía. En el sector público la criptografía se utiliza para garantizar la seguridad de ciertos elementos de los servicios de gobierno electrónico. Actualmente el gobierno no limita, orienta ni promueve el desarrollo, la elección o el uso de métodos y productos criptográficos, y no controla las importaciones o exportaciones de estos productos. Costa Rica no tiene normas relativas al acceso legal a claves en texto claro o criptográficas de datos cifrados, ni normas relativas a la responsabilidad de las personas y entidades que ofrecen servicios criptográficos o poseen o tienen acceso a claves criptográficas.

Sin embargo, varias leyes y reglamentos asociados con la criptografía están alineados con la Recomendación. La Ley N° 8454 de Certificados, Firmas Digitales y Documentos Electrónicos (2005) ayuda a promover la confianza en los métodos criptográficos y su elección. El Decreto Ejecutivo N° 33018, Reglamento de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (2006) ayuda a promover la confianza en la criptografía y sus estándares. La Ley N° 8968 de Protección de la persona frente al tratamiento de sus datos personales (2011) protege los datos personales y la privacidad. La

Ley N° 8642, Ley General de Telecomunicaciones (2008), está alineada con la protección de datos; así como la Ley N° 4573 (que agrega los Artículos 196 BIS, 217 BIS y 229 BIS al Código Penal), Ley para reprimir y sancionar los delitos informáticos. Los procesos judiciales en Costa Rica respaldan el acceso legal y la responsabilidad.

## 7. AUTENTICACIÓN ELECTRÓNICA

### 7.1. Políticas

La Ley N° 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, de 2004, y sus reglamentos establecen la política de Costa Rica en materia de firmas electrónicas. El Sistema Nacional de Certificación Digital (SNCD) del MICITT tiene una Política de Certificados (CP) que reúne las reglas de los certificados electrónicos y las firmas digitales para la jerarquía nacional de certificadores registrados.

El objetivo de Costa Rica es usar plataformas de gobierno electrónico, comercio electrónico y banca electrónica mediante el desarrollo de un entorno electrónico digitalmente seguro y legalmente válido. Con el fin de mejorar la calidad y la eficiencia de las relaciones entre el gobierno, las empresas y los ciudadanos, la política de firmas electrónicas y autenticación electrónica aporta certeza respecto de la identidad de los usuarios y los compromisos de todas las partes.

#### *Marco jurídico y regulatorio*

La Ley N° 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, de 2005, dispone la base jurídica para la emisión y uso de certificados de firma digital en Costa Rica que:

- Garantiza que los documentos electrónicos firmados digitalmente tengan el mismo valor legal que los documentos con firmas manuscritas tradicionales y que los documentos electrónicos tengan el mismo valor legal que los documentos en papel.
- Exige que las entidades que emiten certificados digitales se registren ante la Dirección de Certificadores de Firma Digital (DCFD) del MICITT y cumplan los estándares de operación segura.
- Se aplica a todo tipo de transacciones y actos legales, públicos o privados (a menos que la ley disponga lo contrario, o que la naturaleza y los requisitos comerciales específicos sean incompatibles).
- Autoriza expresamente al Estado y a todas las entidades públicas a utilizar certificados, firmas digitales y documentos electrónicos en sus respectivas áreas de competencia.
- Contiene los mecanismos específicos para reconocer mecanismos de certificación digital del extranjero, incluidas las firmas digitales (artículos 13 a 20).

Además, la Ley N° 8923 de Aprobación de la Adhesión a la Convención para la Eliminación del Requisito de Legalización para los Documentos Públicos Extranjeros, de 2011, adoptó la Convención de la Apostilla, que especifica las modalidades a través de las cuales un documento emitido en uno de los países firmantes (incluida la apostilla electrónica) puede certificarse para fines legales en todos los demás estados signatarios.

El Reglamento de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, el Decreto Ejecutivo N° 33018 (2006) y la Modificación del Reglamento de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, el Decreto Ejecutivo N° 34890 (2008) complementan la Ley N° 8454. En particular, crean un órgano oficial de múltiples partes interesadas llamado Comité Asesor de Políticas (CAP) que asesora a la DCFD. El CAP incluye representantes de la Cámara de Tecnologías de Información y Comunicación (CAMTIC), instituciones académicas públicas y otros.

Finalmente, la Directriz Presidencial N° 067-MICITT-H-MEIC, Masificación de la Implementación y el Uso de la Firma Digital en el Sector Público Costarricense (2014), exige que cada servicio nuevo de gobierno electrónico creado desde que se emite la directriz en 2014 debe implementar un método de autenticación seguro basado en un certificado digital (artículo 3).

### ***Responsabilidades y facultades***

Las principales entidades que participan en el desarrollo y la implementación de la política de autenticación electrónica en Costa Rica son:

- El MICITT, que aporta el liderazgo, a través de la Dirección de Certificadores de Firma Digital (DCFD), en materia de firmas y autenticación electrónica basada en certificaciones digitales. El MICITT es responsable del desarrollo de la política de firma electrónica en colaboración con el Comité Asesor de Políticas (CAP).
- La DCFD, dependencia del MICITT, está a cargo de la implementación de las políticas nacionales y su cumplimiento, y administra la Autoridad Certificadora Raíz.
- El Comité Asesor de Políticas (CAP), el organismo oficial conformado por múltiples partes interesadas que asesora a la DCFD en la implementación de las políticas. El CAP incluye representantes de la Cámara de Tecnologías de Información y Comunicación (CAMTIC), instituciones académicas públicas y otros.
- El Banco Central de Costa Rica (BCCR), que aloja la única Autoridad de Certificación (CA) reconocida por el Sistema Nacional de Pagos Electrónicos (SINPE), emite y hace cumplir las políticas relativas a sus propios servicios.

## **7.2. Implementación**

En agosto de 2009 Costa Rica lanzó su Sistema de Certificación Digital, diseñado para promover transacciones en línea más seguras. El Banco Central de Costa Rica (BCCR) procedió a emitir las firmas digitales. Los principales objetivos del sistema son aumentar el uso de firmas digitales en instituciones del sector financiero y desarrollar aplicaciones que puedan utilizar los certificados emitidos. El proceso de emisión de certificados incluye profesionales de seguridad de la información y abogados, entre otros.

Actualmente el Banco Central de Costa Rica es una Autoridad Certificada para emitir certificados de firma digital para individuos (CA SINPE - personas físicas) y entidades (CA SINPE - personas jurídicas), y también brinda servicios de sellado de tiempo (TSA SINPE). El uso de certificados fortalece los servicios en línea del sector público porque garantiza que se realicen transacciones en línea más seguras. Entre las características del sistema implementado están:

- Usabilidad: la Política de certificados (CP) requiere que, para facilitar su adopción, todas las soluciones de certificados tengan mecanismos integrales y soporte al usuario.
- Idoneidad: la CP establece que las autoridades de certificación y los organismos similares deben adoptar las mejores prácticas al implementar la solución.
- Continuidad comercial: la CP requiere que las autoridades de certificación tengan una Política de continuidad comercial.

- Educación y concienciación: la DCFD trabaja continuamente en campañas en los medios y actividades públicas para aumentar la concientización y la adopción. Establecido en el PNCTI.
- Divulgación: la CP establece requisitos específicos en materia de divulgación de información técnica que las autoridades de certificación deben cumplir.
- Gestión de reclamaciones: La Ley N° 8454 exige que las Autoridades de Certificación (CA) respondan a las reclamaciones de los usuarios y que estas pueden ser elevadas a la DCFD.
- Auditorías y evaluaciones independientes: Costa Rica está revisando actualmente sus políticas en materia de auditorías independientes de acuerdo con sus leyes y reglamentos.
- Enfoques entre jurisdicciones: Las leyes pertinentes en Costa Rica abarcan el reconocimiento de servicios extranjeros.
- Estándares: Costa Rica adopta estándares internacionales para cada elemento de su solución, según lo establecido en la CP.

Las leyes y los respectivos reglamentos se implementan y hacen cumplir mediante el registro, el proceso de aprobación y las actividades de auditoría que ejecuta la DCFD.

La DCFD trabaja con instituciones públicas y privadas para desarrollar nuevas soluciones de gobierno electrónico y comercio electrónico que implementen certificados digitales. La DCFD también promueve la adopción entre los ciudadanos a través de presentaciones públicas en todo Costa Rica, de información en su sitio web (<http://mifirmadigital.go.cr>, donde el gobierno enumera los sistemas que aceptan firma digital) y a través de campañas de publicidad en línea en las redes sociales.

La Ley contempla acuerdos transfronterizos en materia de reconocimiento de certificados digitales. Si bien Costa Rica aún no ha celebrado este tipo de acuerdos, la DCFD está explorando oportunidades para celebrar acuerdos transfronterizos a través de reuniones con otras autoridades de certificación digital en la región, en particular en Brasil, Panamá y Perú.

### 7.3. Seguimiento y evaluación

Se recopilan datos sobre los servicios que implementan certificados digitales, el número de ciudadanos con certificados digitales y el porcentaje de funcionarios públicos que han sido capacitados en el uso de firmas digitales. Los objetivos de la política de firma digital se definen en el Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021 (PNCTI) y en el Plan Operativo Anual del Ministerio. El cumplimiento de los objetivos de firma electrónica y autenticación electrónica es evaluado por la Oficina de Planificación del MICITT, por el Ministerio de Planificación Nacional y Política Económica (MIDEPLAN) y por la Contraloría General de la República.

### 7.4. Evaluación

#### ***Recomendación del Consejo en materia de Autenticación Electrónica [OCDE/LEGAL/0353]***

Costa Rica cuenta con medidas para fomentar el uso de la firma electrónica y métodos de autenticación electrónica. El gobierno lidera la adopción de la firma electrónica y la autenticación electrónica y concientiza sobre el uso de métodos de autenticación electrónica, especialmente para los servicios de gobierno electrónico. El marco jurídico y regulatorio vigente y las prácticas establecidas en la Política de Certificación del Sistema Nacional de Certificación Digital (SNCD) son coherentes con los principios contenidos en los

instrumentos de la OCDE relativos a la autenticación electrónica, entre ellos: neutralidad tecnológica; buenas prácticas comerciales; interoperabilidad y compatibilidad comercial, legal y técnica a través de fronteras; y sensibilización de todos los participantes.

## 8. SPAM

### 8.1. Políticas

Costa Rica tiene un marco interno que abarca el correo no deseado (*spam*) y coopera con las autoridades extranjeras en esta materia.

#### *Marco jurídico y regulatorio*

El marco jurídico de Costa Rica procura proteger a los ciudadanos ante las comunicaciones no deseadas o no solicitadas mediante el establecimiento del derecho a no recibir información no solicitada, normas sobre el procesamiento de datos personales y la consideración de las conductas relacionadas con el spam como delitos informáticos.

- La Ley N° 8642, Ley General de Telecomunicaciones, regula las comunicaciones no solicitadas. El artículo 42 detalla las cláusulas que se consideran abusivas. El artículo 44 establece el derecho de los ciudadanos a no recibir información no solicitada y exige que se suspenda el envío de información cuando los ciudadanos que previamente habían dado su autorización ya no desean recibir las comunicaciones.
- La Ley N° 8968 de Protección de la persona frente al tratamiento de sus datos personales estipula los principios y la regulación del procesamiento de datos personales, que son violados por el correo no deseado cuando los datos de contacto se utilizan para fines distintos de la transacción para la cual se recopilaron los datos. La Ley N° 8968 exige que las bases de datos disponibles públicamente se registren ante la Agencia de Protección de Datos de los Habitantes (PRODHAB) y exige que se protejan los datos confidenciales.
- El Código Penal modificado (Ley N° 9048) actualiza los delitos informáticos, incluidos el *phishing*, la instalación de software malicioso, la falsificación de sitios web y el espionaje informático, actividades a menudo asociadas con el correo no deseado.

También están vigentes las siguientes regulaciones:

- El Reglamento de la Ley de Protección de la persona frente al tratamiento de sus datos personales, Decreto Ejecutivo 37554-JP.
- El Reglamento sobre medidas para proteger la privacidad de las comunicaciones, Decreto Ejecutivo 35205-MINAE.
- El Reglamento de Tarjetas de Crédito y Débito, Decreto Ejecutivo 35867-MEIC, incluye un capítulo que establece las reglas relativas al derecho a la protección de datos de los usuarios de los servicios financieros. El artículo 23 estipula los derechos de acceso, rectificación y cancelación. El artículo 24 establece el procedimiento para la rectificación y eliminación de usuarios de datos de servicios financieros, y el artículo 25 contempla la posibilidad de que los titulares de tarjetas rechacen la publicidad emitida por los emisores de tarjetas de crédito y débito.

El Decreto Ejecutivo del 25 de octubre de 2017, que contiene una reforma parcial al Reglamento de la Ley N° 7472 de Promoción de la Competencia y Defensa Efectiva del Consumidor, prohíbe a las empresas enviar comunicaciones electrónicas no solicitadas por cualquier medio. Exige que los comerciantes desarrollen e implementen procedimientos efectivos y fáciles de usar para que las personas consumidoras elijan si desean recibir o no mensajes comerciales, y que cuando decidan no recibirlos, se respete su decisión de inmediato. El Decreto Ejecutivo estipula que, para que una comunicación comercial no se

considere no solicitada, el consumidor debe haber expresado su consentimiento antes de recibirla.

El Decreto Ejecutivo también establece un mecanismo de coordinación entre la DAC y la Superintendencia de Telecomunicaciones (SUTEL), según el cual la SUTEL puede referir a la CNC los casos que presenten indicios de que una empresa es responsable de enviar comunicaciones no solicitadas o de incluir la suscripción automática o engañosa a bienes o servicios sin el consentimiento expreso del consumidor (excepto en el caso de operadores o proveedores de servicios de telecomunicaciones).

El objetivo de estas regulaciones contra las comunicaciones no deseadas es constituir una política integral contra el *spam* que abarque a los operadores de servicios de telecomunicaciones, los proveedores de servicios de telemarketing y marketing en línea y las empresas de ventas directas que utilizan este tipo de prácticas. Además, la SUTEL está trabajando en la aprobación de un Reglamento de Protección del Usuario que incluye disposiciones relacionadas con las comunicaciones no solicitadas enviadas por operadores o proveedores de servicios de telecomunicaciones.

La PRODHAB, la SUTEL, la Corte Suprema de Justicia, la Comisión Nacional del Consumidor (CNC), las asociaciones de personas consumidoras y el sector privado se encargan de exigir el cumplimiento de la política de comunicaciones no deseadas en Costa Rica.

## 8.2. Implementación y aplicación

La SUTEL exige el cumplimiento de la política de comunicaciones no solicitadas utilizando un procedimiento de reclamación descrito en los artículos 47 y 48 de la Ley N° 8462 en relación con los operadores de telecomunicaciones. En ese caso, las personas consumidoras pueden solicitar eliminar sus nombres de la base de datos y detener cualquier tipo de comunicación no deseada.

Además, los órganos gubernamentales costarricenses cooperan con entidades del sector privado para proteger a las personas consumidoras frente al correo no deseado; por ejemplo, a través de actividades de capacitación conjunta con entidades del sector empresarial y agencias calificadoras de crédito.

### *Cooperación internacional*

Costa Rica coopera e intercambia información con autoridades extranjeras que fiscalizan el *spam* a través de foros internacionales, entre ellos la Red Iberoamericana de Protección de Datos, la Red Internacional de Protección del Consumidor y Aplicación de la Ley (ICPEN por sus siglas en inglés) y el Consejo Centroamericano de Protección al Consumidor (CONCADECO).

### *Desafíos*

Desde la perspectiva de la protección de datos personales, las políticas se apoyan en diferentes fuentes de legislación nacional, pero requieren un mayor desarrollo, particularmente en relación con la coordinación entre el gobierno y las partes involucradas.

Hasta octubre de 2017 no existía un mecanismo eficiente y expedito en Costa Rica para dejar de recibir comunicaciones no deseadas; por ejemplo, cuando un consumidor previamente aceptó o solicitó comunicaciones pero ya no desea recibirlas. Se prevé que esta situación cambiará con el reciente Decreto Ejecutivo que contiene una reforma parcial al Reglamento de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor.

### 8.3. Seguimiento y evaluación

La PRODHAB supervisa la implementación de las políticas de protección de datos personales, incluidos los aspectos relacionados con el correo no deseado, mediante la recopilación de información sobre la cantidad de bases de datos registradas de datos personales y la cantidad de reclamaciones presentadas. Con base en esta información la Agencia prepara informes mensuales y anuales de evaluación con el objetivo de mejorar la política.

### 8.4. Evaluación

***Recomendación del Consejo en materia de cooperación transfronteriza en la aplicación de las leyes contra las comunicaciones no solicitadas [OCDE/LEGAL/0344]***

Este instrumento está bajo la responsabilidad conjunta del Comité de Políticas para la Economía Digital (CDEP) y el Comité de Políticas del Consumidor (CCP). La implementación de esta Recomendación por parte de Costa Rica también se analiza en el informe sobre Políticas de los Consumidores en Costa Rica.

La política de Costa Rica para combatir las comunicaciones no solicitadas se limitaba hasta hace poco a cuestiones que se tratan en el contexto de la privacidad y la protección de datos, con cooperación transfronteriza en la aplicación de las leyes limitada a casos que implican la violación de la privacidad o los de derechos a la protección de datos y con una cooperación con entidades del sector privado posible en principio pero no formalizada.

Un nuevo Decreto Ejecutivo que entró en vigor el 25 de octubre de 2017 prohíbe a las empresas enviar comunicaciones electrónicas no solicitadas y les exige desarrollar e implementar procedimientos efectivos y fáciles de usar que les permitan a las personas consumidoras elegir si desean recibir mensajes comerciales. Se espera que ayude a garantizar una política integral contra las comunicaciones no solicitadas en Costa Rica.

## 9. LAS DECLARACIONES SOBRE LA INTERNET Y LA ECONOMÍA DIGITAL

### 9.1. Políticas

El Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) de Costa Rica, emitido en 2015, destaca varias de las prioridades de la Declaración de Seúl para el Futuro de la Economía de Internet y de la Declaración sobre la economía digital: innovación, crecimiento y prosperidad social (“Declaración de Cancún”). El PNDT aspira a “[t]ransformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones; de forma segura, responsable y productiva.” El PNDT tiene tres pilares: *i*) inclusión digital: acceso universal, servicio universal y solidaridad en los proyectos de telecomunicaciones y TIC, así como una mejor calidad de los servicios de telecomunicaciones prestados al público, incluida la expansión de la oferta de servicios asequibles e innovadores; *ii*) economía digital: crear un entorno favorable que permita la convergencia hacia la digitalización y la innovación asociada a ella; y *iii*) gobierno transparente y electrónico, incluidos los temas de seguridad digital.

En otras secciones de este informe se discuten algunas de las políticas incluidas en la Declaración de Seúl para el Futuro de la Economía de Internet [[OECD/LEGAL/0366](#)] y en la Declaración sobre la economía digital: Innovación, crecimiento y prosperidad social (Declaración de Cancún) [[OCDE/LEGAL/0426](#)], entre ellas las secciones sobre el desarrollo de banda ancha, la información en el sector público, las TIC y el medio ambiente, los principios de la formulación de políticas de Internet; la privacidad, la gestión de riesgos de seguridad digital, la protección de la infraestructura de información crítica, la protección de la niñez en línea; y también en el informe independiente sobre Políticas de los Consumidores en Costa Rica.

Esta sección se centra en una visión general de las políticas de Costa Rica orientadas a:

- estimular la innovación digital y la creatividad (una recomendación incluida tanto en la Declaración de Seúl como en la Declaración de Cancún);
- desarrollar las habilidades necesarias para participar en la economía digital y estimular las oportunidades de empleo creadas por la economía digital (recomendación incluida en el Declaración de Cancún);
- asegurar que la economía de internet sea verdaderamente global (recomendación incluida en el Declaración de Seúl).

El Viceministerio de Telecomunicaciones del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) coordina, guía y formula políticas específicas para promover y fomentar el desarrollo de la ciencia y la tecnología en general con el fin de garantizar el derecho de los ciudadanos al acceso a los servicios de telecomunicaciones, así como el seguimiento y la evaluación del Plan Nacional de Desarrollo de las Telecomunicaciones. Además, el MICITT apoya financieramente actividades científicas y tecnológicas que contribuyan a realizar intercambios científicos y técnicos con otros países, o que estén vinculados a los objetivos nacionales de desarrollo. El MICITT ha estado otorgando estímulos e incentivos financieros a actores privados y públicos, nacionales y extranjeros y a centros de educación superior, incluidas universidades, para aumentar la capacidad de Costa Rica en ciencia y tecnología.

La Superintendencia de Telecomunicaciones (SUTEL) también promueve la competencia en los mercados de telecomunicaciones. El Ministerio de Economía, Industria y Comercio (MEIC) desarrolla políticas regulatorias en materia económica y social para proteger a las personas consumidoras y fomentar la competitividad en el mercado. El Ministerio de Comercio Exterior (COMEX) diseña políticas relacionadas con el comercio internacional y dirigidas a promover la participación de las empresas costarricenses en la economía de internet a través de acuerdos comerciales internacionales.

Las instituciones del sector público forman alianzas para implementar políticas con otras organizaciones que, aunque privadas, tengan un propósito público. Estas incluyen la Coalición Costarricense de Iniciativas de Desarrollo (CINDE) y la Promotora del Comercio Exterior de Costa Rica (PROCOMER). La primera tiene un papel de liderazgo en la atracción de empresas de servicios y de alta tecnología para que inviertan en Costa Rica, incluidas las que forman parte de la economía de internet; y la segunda tiene entre sus funciones promover las industrias exportadoras, como todas aquellas empresas que desean exportar para participar en la economía de internet.

Las partes interesadas no gubernamentales, incluidas empresas y la sociedad civil, desempeñan una función importante en el fomento de una economía digital innovadora en Costa Rica. CAMTIC, aceleradores y fondos de inversión conforman un ecosistema cada vez más favorable a la innovación digital en Costa Rica.

## 9.2. Implementación

### *Innovación y creatividad digital*

Los dos tipos principales de políticas para promover la innovación y la creatividad digital en Costa Rica son las que facilitan las operaciones comerciales y las que promueven la innovación en las empresas de tecnología.

Para facilitar las operaciones comerciales:

- Costa Rica ha tratado de fortalecer el entorno empresarial relacionado con la economía digital a través de mejoras regulatorias. Una reforma en curso que cabe destacar es la digitalización y simplificación de los procedimientos administrativos para las empresas. La implementación de *CrearEmpresa* a principios de 2012, un sistema digital para el registro de personas jurídicas marcó un hito importante en la simplificación de los procedimientos para empezar una empresa. *CrearEmpresa* actúa como una ventanilla única que interconecta a todos los órganos de gobierno que participan en el registro de empresas. Registrar una empresa en Costa Rica ahora lleva una hora en lugar de varios días, y cuatro etapas se han agrupado en una sola.
- El MEIC también ha venido tomando medidas para digitalizar los procedimientos. Por ejemplo, el programa de reglamentación electrónica *Costa Rica Facilita Negocios* es una plataforma digital que resume los pasos que deben seguir los inversores para crear una empresa en Costa Rica. Fue lanzado en 2010 con el apoyo financiero del Programa de las Naciones Unidas para el Desarrollo (PNUD) y el gobierno de Luxemburgo, y con la asistencia técnica de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD). Otras iniciativas importantes incluyen la mejora de la recaudación fiscal y el establecimiento de una ventanilla única para el comercio exterior, llamada VUCE (*Ventanilla Única de Comercio Exterior*).
- La implementación del Sistema Nacional de Pagos Electrónicos (SINPE) por parte del Banco Central de Costa Rica también facilita los negocios al permitir realizar transferencias digitales de dinero en tiempo real, incluso de un número de teléfono a otro y con cuentas en diferentes bancos. Las transferencias digitales de dinero en Costa Rica se multiplicaron por cinco en los últimos seis años hasta llegar a CRC 137 mil millones (casi USD 252 millones) en 2015, según la Superintendencia de Telecomunicaciones (SUGEF).

Para promover la innovación en las empresas:

- El Programa de Innovación y Capital Humano para la Competitividad, financiado por el Banco Interamericano de Desarrollo desde 2013, ha estimulado el crecimiento de la productividad al apoyar la innovación y fortalecer el capital humano en sectores estratégicos. Es administrado por el MICITT con el apoyo de COMEX. El programa, que apunta a estimular la innovación en las empresas costarricenses y a fomentar los emprendimientos basados en nuevas tecnologías, ofrece asistencia técnica a pequeñas y medianas empresas (PYME) y a emprendedores de base tecnológica y cofinancia proyectos de innovación para emprendedores o PYMES.
- En términos de políticas de comercio internacional, Costa Rica ha tratado de incluir el comercio electrónico en sus compromisos comerciales. Por ejemplo, ha apoyado el desarrollo de una agenda de discusión sobre comercio electrónico en la Organización Mundial de Comercio (OMC) y una moratoria que establece que los Miembros de la OMC no impondrán derechos de aduana a las transmisiones electrónicas.

### ***Desarrollo de habilidades***

Fortalecer y desarrollar las habilidades en TIC es uno de los objetivos del PNDDT a través de su módulo de 'alfabetización digital'. Las acciones para implementar este objetivo incluyen capacitar a personas que previamente no han utilizado la internet, en cooperación con las comunidades locales; ayudar a las personas a que hagan un uso eficaz, avanzado y seguro de internet; alentar a las personas jóvenes a estudiar profesiones relacionadas con las TIC; y promover el aprendizaje permanente en el entorno digital.

### ***Garantizar que la economía de internet sea verdaderamente global***

Costa Rica también tiene políticas cuyo objetivo es garantizar que la economía de internet sea verdaderamente global. Por ejemplo, el eje de inclusión digital del PNDDT apoya un mayor acceso a internet y las TIC relacionadas a ella y el desarrollo de servicios mejorados para personas con discapacidades y necesidades especiales. Además, los capítulos de comercio electrónico de los acuerdos comerciales ponen un importante énfasis en promover la cooperación transfronteriza y el intercambio de información entre los gobiernos en las áreas de ciberseguridad, combatir las comunicaciones no solicitadas y proteger la privacidad y a las personas consumidoras y las personas menores de edad.

### ***Facilitar la convergencia***

También cabe señalar que Costa Rica fomenta la adopción de IPv6 a través de los objetivos del PNDDT y de la Directriz N° 049-MICITT, que establece plazos para la implementación del protocolo de Internet IPv6 en el sector público costarricense. La Sección dedicada al desarrollo de la banda ancha detalla otras iniciativas de Costa Rica en esta área.

## **9.3. Seguimiento y evaluación**

El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) le da seguimiento al PNDDT y al PNCTI. MIDEPLAN le da seguimiento al PND. El Ministerio de Hacienda hace el seguimiento del presupuesto en relación con la ejecución de los objetivos.

#### 9.4. Evaluación

*Declaración para el Futuro de la Economía de Internet (Declaración de Seúl) [[OECD/LEGAL/0366](#)] y Declaración sobre la economía digital: Innovación, crecimiento y prosperidad social (Declaración de Cancún) [[OCDE/LEGAL/0426](#)]*

Costa Rica se adhirió a la Declaración de Seúl el 16 de octubre de 2013 y a la Declaración de Cancún el 23 de junio de 2016. El Plan Nacional de CTI 2015-2021 (PNCTI) y otros programas fomentan la innovación y la creatividad en el desarrollo, el uso y la aplicación de internet y fortalecen el capital humano y el espíritu empresarial en las tecnologías digitales. El desarrollo de las habilidades necesarias para participar en la economía digital es una prioridad en el PNDT de Costa Rica en su eje de inclusión digital. Las políticas de Costa Rica en materia de protección de datos personales y gestión de riesgos de seguridad digital fortalecen la confianza y la seguridad. La política de banda ancha de Costa Rica facilita la convergencia de redes digitales, dispositivos, aplicaciones y servicios. El Comité de Políticas de los Consumidores evalúa las políticas para las personas consumidoras en Costa Rica, incluso en los mercados de telecomunicaciones.

## 10. INFORMACIÓN DEL SECTOR PÚBLICO

### 10.1. Políticas

Dos líneas principales de políticas enmarcan el acceso y el uso de la información del sector público (ISP): el compromiso firme de abrir el gobierno y los datos relacionados al gobierno abierto, y el contrapeso entre privacidad y protección de datos personales. Si bien Costa Rica no tiene una política explícita de ISP, hay un Proyecto de Ley de Acceso a la Información Pública, el N° 20.361, en proceso parlamentario.

La base del desarrollo de políticas en Costa Rica es el Plan Nacional de Desarrollo "Alberto Cañas Escalante" 2015-2018 (PND).<sup>6</sup> El tercer pilar del PND define la estrategia nacional de gobierno abierto (ENGA).<sup>7</sup> Los datos de gobierno abierto son una de las características del eje de Transparencia y Acceso a la Información Pública de la ENGA, cuyo objetivo es implementar una cultura de transparencia y garantizar el acceso a la información pública como un derecho humano.

El PND define las prioridades y los objetivos nacionales para impulsar el crecimiento económico y el empleo de calidad; la lucha contra la pobreza y la reducción de la desigualdad; y un gobierno abierto y transparente que combate la corrupción. Su objetivo es avanzar hacia una sociedad basada en la equidad, el conocimiento, la innovación, la competitividad, la transparencia y el desarrollo sostenible. Las estrategias sectoriales son: trabajo y seguridad social; desarrollo humano e inclusión social; salud, nutrición y deporte; educación; vivienda y asentamientos humanos; cultura y juventud; desarrollo agrícola y rural; finanzas públicas, supervisión monetaria y financiera; economía, industria y comercio; comercio exterior; turismo; transporte e infraestructura; ciencia, tecnología y telecomunicaciones; política internacional; medio ambiente, energía, mares y ordenamiento territorial; y seguridad ciudadana y justicia.

La ENGA se elaboró en 2017 mediante el Decreto Ejecutivo N° 40199-MP que establece la apertura de los datos públicos<sup>8</sup> y la correspondiente Directriz N° 074-MP de Apertura de Datos Abiertos; el Decreto Ejecutivo N° 40200-MP-MEIC-MC sobre Transparencia y Acceso a la Información Pública<sup>9</sup> y la correspondiente Directriz N° 073-MP-MEIC-MC sobre Transparencia y Acceso a la Información Pública.

La regulación del acceso a la información pública se distribuye entre diferentes órganos reguladores, de conformidad con los artículos 27 y 30 de la Constitución Política.<sup>10</sup> El artículo 27 garantiza la libertad de solicitar, en forma individual o colectiva, información de cualquier servidor público o entidad oficial y el derecho a obtener una pronta resolución. El artículo 30 garantiza el acceso libre a los departamentos administrativos para obtener información sobre asuntos de interés público. Se excluyen los secretos de estado.

**Gobierno abierto** Costa Rica se unió a la Asociación de Gobierno Abierto (llamada anteriormente Alianza para el Gobierno Abierto) en 2012. En 2015, el gobierno y la Red Ciudadana por un Gobierno Abierto establecieron la Comisión Nacional de Gobierno Abierto (CNGA).<sup>11</sup> Esta Comisión permanente está presidida por el Ministro o Viceministro de la Presidencia, y está compuesta por los Ministros o Viceministros de: Ciencia, Tecnología y Telecomunicaciones; Planificación Nacional y Política Económica; Hacienda; Justicia y Paz; y dos representantes de la sociedad civil, un representante del Consejo Nacional de Rectores y un representante de la Unión Costarricense de Cámaras y Asociaciones del Sector Empresarial Privado (UCCAEP). Los miembros participantes son renovados cada dos años. La CNGA comenzó a reunirse en agosto de 2015 y el Plan de Acción de Gobierno Abierto está en vigor desde octubre de 2015. Varias dependencias del Poder Judicial son responsables de su cumplimiento, incluida la Corte Suprema de Justicia, el Consejo Supremo, la Comisión de Accesibilidad y el Comité de Gestión Tecnológica. La ISP no se distingue por separado. La política de ISP se deriva de la estrategia y los compromisos de Gobierno Abierto.

El objeto de la CNGA es: "fomentar los principios del Gobierno Abierto en la Administración Pública de Costa Rica, principios que se manifiestan en: mejorar los niveles de transparencia, garantizar el acceso democrático a la información pública, promover y facilitar la participación ciudadana e impulsar la generación de espacios de trabajo colaborativo interinstitucional y ciudadano; mediante la innovación y aprovechando al máximo las facilidades que brindan las Tecnologías de la Información y Comunicación (TIC)."

De acuerdo con el artículo 30 de la Constitución, las áreas que abarca comprenden la gama completa de información administrativa necesaria para el funcionamiento del gobierno: "el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de estado." Esto da acceso, entre otros, a la información recopilada en los diferentes archivos nacionales, registros judiciales, archivos del sistema penitenciario, el Fondo de Seguridad Social, el Sistema de Estadística Nacional, el control y la supervisión generales de las instituciones y la información fiscal. Sin embargo, no se incluyen para su acceso y uso áreas clave de ISP; por ejemplo: datos geoespaciales, datos catastrales, datos meteorológicos, datos científicos y técnicos y datos operativos similares, así como contenido digital como, por ejemplo, archivos, bibliotecas, museos y obras de arte en el dominio público.

Actualmente hay dos formas de acceder a los datos de gobierno abierto: solicitar información a la CNGA a través de [gobiernoabierto@presidencia.go.cr](mailto:gobiernoabierto@presidencia.go.cr); o mediante el mecanismo establecido en el Decreto Ejecutivo N° 40200-MP-MEIC-MC, según el cual las instituciones designan a un Oficial de Acceso a la Información que será el responsable de recibir, gestionar y responder las consultas en un plazo de diez días hábiles, de conformidad con la Ley General de Administración Pública. Costa Rica también está en el proceso de nombramiento de una Comisión Nacional de Datos Abiertos que proveerá un tercer mecanismo para recibir solicitudes de datos. Todos difieren en la cobertura de la información del sector público.

**Protección de los datos personales:** La compensación de la protección de los datos personales está bien desarrollada, pero su objetivo difiere de garantizar el acceso y el uso de la información del sector público. La protección de los datos personales está estipulada en la Ley N° 8968.<sup>12</sup> La Ley N° 8454 de Protección de la Persona frente al tratamiento de sus datos personales, creó la Agencia de Protección de Datos de los Habitantes (PRODHAB). Las atribuciones de la Agencia se detallan en el artículo 16, incisos A-J. La PRODHAB tiene una función "pasiva", es decir, reacciona en casos específicos en los que la privacidad de los datos personales se ve comprometida, y no tiene funciones "activas" en relación con la información del sector público. El Decreto Ejecutivo N° 40200-MP-MEIC-MC (artículo 17) de 2017 enumera la información pública accesible.

### ***Marco jurídico y regulatorio***

La ENGA es el elemento principal de la estrategia de ISP de Costa Rica. La ENGA fue el resultado de un proceso colectivo dedicado a consolidar y poner en funcionamiento una red de reformadores de Gobierno Abierto institucionales y de la sociedad civil. En conjunto con la CNGA, esta red implementa políticas, proyectos y acciones, así como los objetivos prioritarios de la Estrategia para el gobierno central.

Entre las metas y acciones regulatorias de la ENGA están:

- **Política de datos abiertos.** Establecer las bases técnicas y regulatorias para la apertura de datos, que incluyen: publicaciones frecuentes, neutralidad tecnológica, interoperabilidad de datos y estrategias de comunicación, y establecer formatos y estándares mínimos de contenido que le garanticen el acceso a los usuarios y su comprensión.<sup>13</sup>
- **Lograr la adopción del Proyecto de Ley de Transparencia y Acceso a la Información Pública (N° 20.361).** Este proyecto, más amplio que los Decretos Ejecutivos de 2017, propone hacer obligatorio que las municipalidades y las instituciones autónomas y semiautónomas apliquen el Decreto Ejecutivo sobre Apertura de Datos N° 40199-MP. El Proyecto de Ley de Acceso a la Información Pública N° 20.361 actualizado amplía el Proyecto de Ley N° 19.113.
- **Transparencia y acceso a la información pública.** El Decreto Ejecutivo sobre Transparencia y Acceso a la Información Pública N° 40200-MP-MEIC-MC garantiza el derecho de acceso a la información pública.
- **Directorio de información de perfiles de las instituciones públicas.** El objetivo es desarrollar una plataforma interactiva que provea información actualizada sobre las instituciones públicas de manera integral.
- **Diseño de un plan piloto para la gestión de documentos y la administración de archivos.** El objetivo es implementar un plan piloto único para la gestión de documentos y la gestión de archivos en el Sistema Nacional de Archivos.
- **Índice de transparencia del sector público (Defensoría de los Habitantes).** El índice ofrece una visión general de la transparencia de los sitios web del sector público, incluido el acceso abierto a la información, la rendición de cuentas y la participación ciudadana.

El proyecto de Ley de Transparencia y Acceso a la Información Pública (N° 19.113) inicial se basó en una propuesta de la sociedad civil: "Costa Rica Íntegra". El texto fue desarrollado por la subcomisión de la CNGA sobre Transparencia y Acceso a la Información (ver más adelante) y mediante consulta pública. El proyecto está en la Asamblea Legislativa.

El Ministro de Comunicaciones y el Ministro de la Presidencia están promoviendo una actualización de la Ley de acceso a la información pública (N° 20.361). Luego de la revisión del Proyecto de Ley N° 19.113, el nuevo proyecto de ley incluye adiciones y modificaciones que la CNGA considera necesarias. Se presentó a la Asamblea Legislativa después de la revisión de la CNGA y de realizar consultas.

Las principales diferencias son que el proyecto de ley N° 20.361:

- Establece principios adicionales sobre el acceso a la información pública como derecho humano.
- Con el fin de aumentar la transparencia institucional y la rendición de cuentas, amplía la lista de información pública que se publica de manera obligatoria de 13 a 19 elementos. Esta ampliación está alineada con el Índice de Transparencia del Sector Público que implementó la Defensoría de los Habitantes, a la cual también se le asigna la responsabilidad de garantizar la publicación de esta información.
- Incluye los siguientes artículos:
  - Asistencia a personas con barreras de acceso que incluyen barreras de lenguaje, motoras, físicas, cognitivas, visuales y auditivas.
  - Plazos para responder a las solicitudes de información.

- Formas de proporcionar esta información.
- Excluye el órgano garante establecido por el proyecto de ley N° 19.113 porque requería la creación de una estructura organizativa y de recursos humanos, de infraestructura, materiales y tecnológicos para su funcionamiento eficaz, lo cual resultaría difícil dada la actual situación fiscal y política.

### ***Responsabilidades y facultades***

El Ministerio de la Presidencia (Viceministerio de Asuntos Políticos y Diálogo Ciudadano) y la Asamblea Legislativa lideran las políticas de gobierno abierto y de datos del gobierno abierto. La implementación y la aplicación de ley están a cargo del Ministerio de la Presidencia y la Asamblea Legislativa, en conjunto con la Sala Constitucional, la Contraloría General y PRODHAB.

La Estrategia Nacional de Gobierno Abierto se basa en una amplia consulta con la sociedad civil, la academia, la empresa privada, las instituciones públicas y expertos que participan en la formulación y evaluación de políticas.

**Responsabilidades de la CNGA:** La CNGA tiene un conjunto claro de objetivos políticos y responsabilidades, como se describe en las secciones 1.1 y 1.1.1 (véanse el Decreto Ejecutivo N° 38.994 y los proyectos de ley N° 19.113 y 20.361). Las funciones de la CNGA que establece el artículo 4 son:

- Proponer políticas, directrices, estrategias y planes de acción.
- Promover la cultura de gobierno abierto y la educación de los ciudadanos en esta materia.
- Proponer una metodología de evaluación para la adopción y promoción del Gobierno Abierto.
- Apoyar a las instituciones en la creación de normas para la adopción y promoción del Gobierno Abierto.
- Coordinar las acciones para la implementación de principios de Gobierno Abierto en la gestión pública.
- Proponer metodologías e instrumentos de seguimiento para los planes de acción.
- Dar seguimiento a la implementación de los compromisos de Gobierno Abierto en los planes de acción.
- Emitir informes técnicos y de evaluación sobre el progreso de la implementación de los planes de acción.
- Promover el acercamiento y el intercambio entre diversos actores nacionales.
- Desarrollar relaciones con organizaciones internacionales que promueven e implementan un Gobierno Abierto.
- Coordinar proyectos y actividades y crear sinergias y cooperación.
- Promover instancias que desarrollen conocimiento y capacidades de gestión en materia de Gobierno Abierto.
- Crear subcomisiones dedicadas a actividades y propósitos específicos.
- Colaborar en el establecimiento de la arquitectura de soporte tecnológico del Gobierno Abierto.

**Responsabilidades y facultades de la sociedad civil:** Los sectores académicos, empresariales y de la sociedad civil forman parte de la CNGA y participan en las subcomisiones. Para participar, los representantes de la sociedad civil deben pasar por un proceso de selección y aprobación de la CNGA. Las subcomisiones abarcan: transparencia

y acceso a la información; lucha contra la corrupción; participación ciudadana; desarrollo territorial; y sistemas y plataformas.

**Subcomisión de Participación Ciudadana.** Esta subcomisión difunde información sobre la importancia del Gobierno Abierto y realiza actividades de capacitación. Sus compromisos principales son: *i) capacitación de funcionarios públicos en atención ciudadana* mediante la elaboración del aporte teórico y la metodología de los talleres para funcionarios públicos y la coordinación de talleres con los ministerios e instituciones pertinentes (en 2016 se había capacitado a más de 75 funcionarios públicos y la capacitación de otros 50 estaba programada para septiembre de 2017); *ii) difusión de la política de participación ciudadana*; y *iii) difusión a través del desarrollo de materiales y de comunicación en línea* mediante campañas en redes sociales, *stands* informativos en conferencias, ferias, etc.

**Protocolo para el diálogo con sectores y ciudadanos.** El protocolo se lanzará a través de un Decreto Ejecutivo que está en preparación.<sup>14</sup>

También se han reunido diversos grupos de personas o representantes de diferentes sectores para crear el Plan de Acción colaborativamente. Con el fin de ampliar las observaciones y comentarios se publicó una consulta general en el diario oficial *La Gaceta* y en el sitio web de Gobierno Abierto.

## 10.2. Implementación

### *Leyes y medidas regulatorias*

Los principales instrumentos que permiten acceder a la información pública son la ENGA y el Plan de Acción de Gobierno Abierto que está en vigor desde octubre de 2015, junto con la CNGA. El contrapeso es el fortalecimiento de la protección de los datos personales privados a través de la PRODHAB.

Los derechos y responsabilidades y los perímetros de acción de estas iniciativas están en consulta en la Sala Constitucional. Por ejemplo, los recursos de inconstitucionalidad han fortalecido el derecho de acceso a la información pública y aclarado y delimitado su alcance.

La PRODHAB también ha logrado aclaraciones importantes respecto de sus responsabilidades. El ordenamiento jurídico costarricense exige, primero, cuestionar los criterios de la PRODHAB y, una vez agotados los procedimientos administrativos, la Sala Constitucional puede revisarlos. Un ejemplo es si los casos relacionados con la protección de datos personales deben ir primero a la PRODHAB. La Sala concluyó que la PRODHAB es un mecanismo rápido, oportuno y especializado en garantizar los derechos de los ciudadanos en relación con su vida o sus actividades privadas y otros derechos personales, así como para el tratamiento automatizado o manual de los datos correspondientes.<sup>15</sup>

Otros instrumentos jurídicos relacionados con el acceso a la información son:

- **La Constitución Política de Costa Rica:** Los artículos 27 y 30 garantizan que las personas tengan libre acceso a la información sobre asuntos de interés público. (Véanse las secciones 1.1. y 1.1.1.)
- **La Ley General de Telecomunicaciones (N° 8642):** El artículo 33 estipula que las políticas nacionales de telecomunicaciones deben incorporar una agenda digital, "*como un elemento estratégico para la generación de oportunidades, el aumento de la competitividad nacional y el disfrute de los beneficios de la sociedad de la información y el conocimiento, que a su vez contenga una agenda de solidaridad digital que garantice estos beneficios a las poblaciones vulnerables y disminuya la brecha digital.*"<sup>16</sup>

- La **Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos (N° 8220)** procura facilitar la optimización y simplificación de los procedimientos en las instituciones públicas.<sup>17</sup>
- La **Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (N° 8968)**: El artículo 1 declara: *Esta ley [...] tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.* (Véase también la Sección 1.1)

Los planes nacionales también proveen un marco para las políticas de datos de gobierno abierto:

- El **Plan Nacional de Desarrollo 2015-2018 (PND)** establece el desarrollo de un gobierno transparente y más cercano a los ciudadanos, con la visión de que el gobierno trabaje en estrecha colaboración con la sociedad civil.
- El **Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2018** aspira a *"[t]ransformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones; de forma segura, responsable y productiva."*<sup>18</sup>

### ***Aplicación de la ley***

Aunque actualmente no existen leyes o reglamentos que respalden directamente el acceso a la ISP y su uso, el marco regulatorio vigente tiene como objetivo fortalecer la rendición de cuentas, la participación ciudadana y la transparencia para promover la cultura de acceso a la información y facilitar la lucha contra la corrupción. La Estrategia Nacional de Gobierno Abierto está diseñada para ampliar y mejorar este marco. La Sala Constitucional, la Contraloría General de la República,<sup>19</sup> y la PRODHAB velan por su aplicación, y en 2014 la Casa Presidencial y la Asamblea Legislativa introdujeron nuevas disposiciones legales que aclaran la información que se puede divulgar legalmente.<sup>20</sup> Después de unirse a la Asociación de Gobierno Abierto en 2012 el primer plan de acción se comprometió a fortalecer el acceso a la información, y la Estrategia Nacional de Gobierno Abierto actual apunta a fortalecer todavía más la apertura y el acceso.

**ISP:** El Gobierno ha promovido desde julio de 2014 un Proyecto de Ley sobre Transparencia y Acceso a la Información Pública en la Asamblea Legislativa, el cual ha sido revisado y ampliado en el Proyecto de Ley N° 20.361 que actualmente está promoviendo activamente el Ministerio de Comunicación.

### ***Medidas no regulatorias***

El gobierno dirige el marco de apertura de los datos de gobierno junto con la sociedad civil, la academia y el sector empresarial; por ejemplo, a través de la CNGA, su Subcomisión de Participación Ciudadana y otras subcomisiones que participan por igual en iniciativas no regulatorias de gobierno y datos abiertos.

### ***Implementación, incluidas las medidas no regulatorias***

**Entidades gubernamentales.** La Estrategia Nacional de Gobierno Abierto creó una "Red de Reformadores" compuesta por funcionarios del gobierno central y de instituciones públicas que actúan como los enlaces directos a la Estrategia. Estos funcionarios tienen garantizada su participación en las subcomisiones de la CNGA. Actualmente hay 38 instituciones en la Red, incluidos Ministerios (14), el Banco Central, el Poder Judicial, la Defensoría de los Habitantes, dependencias de gobierno, el Instituto Nacional de Aprendizaje (INA) y la Municipalidad de Palmares.

**Variaciones dentro del gobierno** La implementación del gobierno abierto varía mucho en función de la concienciación sobre el tema, los recursos humanos y tecnológicos, el tamaño y la estructura de la entidad y la capacidad presupuestaria. Hasta ahora, uno de los niveles más altos de implementación de datos abiertos es el logrado por el Programa de Justicia Abierta del Poder Judicial, con el que este se comprometió en octubre de 2013 y afirmó que sería el primero del mundo. La política pública de justicia abierta fue lanzada en 2016 en cooperación con la CEPAL bajo los principios de transparencia, participación y colaboración y con la sociedad civil asumiendo un papel activo en la construcción de políticas. A fines de noviembre de 2016 se celebró un Congreso de Justicia Abierta y empezaron a realizarse visitas en todo el país y consultas en línea.

Entre las instituciones con los niveles más altos de implementación de datos abiertos están:

- Asamblea Legislativa
- Defensoría de los Habitantes
- Contraloría General de la República
- Algunos gobiernos locales (municipalidades)
- Algunas instituciones con margen de mejora son:
  - Gobierno central
  - Poder Judicial
  - Instituciones autónomas
  - Empresas publicas

**Promoción entre empresas y ciudadanos.** Una de las áreas a las que presta mayor atención la ENGA es la participación ciudadana, mediante la promoción del Gobierno Abierto a través de una comunicación constante entre ciudadanos, empresas e instituciones de gobierno. La CNGA se conformó con la participación del sector público, la academia, la sociedad civil y la empresa privadas con el fin de elaborar la Estrategia Nacional. El sector privado ha participado activamente, con representación de la Unión Costarricense de Cámaras y Asociaciones del Sector Empresarial Privado (UCCAEP) en la CNGA.

**Fomento de las asociaciones público-privadas..** La CNGA fomenta las asociaciones público-privadas. Se están promoviendo proyectos de colaboración en áreas que incluyen la mejora y la optimización de los procesos de gestión de la información, la cooperación técnica y la promoción de la reutilización de la información; pero no hay datos disponibles sobre los resultados de estas iniciativas. No existen iniciativas para fomenten el acceso transfronterizo a los datos gubernamentales ni su utilización.

**Acceso a datos y listas de activos.** El objetivo de la Estrategia es que los datos y la información de todas las instituciones públicas estén en un único portal de datos abiertos en <http://gobiernoabierto.go.cr/>, organizado por el Viceministerio de Asuntos Políticos y Diálogo Ciudadano. Este portal también cumple la función de una lista de activos.<sup>21</sup> Sin embargo, las instituciones públicas son invitadas pero no están obligadas a unirse, y por ahora solo hay algunos datos en este portal.

**Condiciones de acceso.** En el marco normativo se toman en consideración el acceso no discriminatorio y las condiciones competitivas de acceso, así como la perspectiva del acceso como un derecho humano. Por ejemplo, se ha propuesto que no se exija presentar una copia de los documentos de identidad personal para acceder a la información pública y para otros procesos públicos, sino tan solo mostrar la identificación original. Además, se están incorporando la neutralidad tecnológica y la escalabilidad al acceso a datos abiertos.

**Reclamaciones y peticiones.** La Ley de Regulación del Derecho de Petición (N° 9097) del 14 de marzo de 2013, regula las peticiones de acceso a la información pública. El artículo 12 estipula que los ciudadanos tienen derecho a recurrir a la Sala Constitucional. Las peticiones no requieren de un abogado.<sup>22</sup> No hay datos oficiales disponibles sobre el número de peticiones o su tasa de éxito.

**Licencias y cargos.** Actualmente no existe licenciamiento, pero se incluye en las propuestas de la Política Nacional de Datos Abiertos de 2017 (véanse los Decretos Ejecutivos mencionados anteriormente). Costa Rica no cobra por proveer ISP. Se espera que los proyectos de ley (N° 19.113 y N° 20.361) no incluyan cargos en sus versiones finales.

**Derechos de autor para facilitar la reutilización.** Se está considerando el acceso abierto con parámetros establecidos para usar la información pública de conformidad con derechos de atribución y difusión. Este enfoque se encuentra en el marco jurídico actual, la Ley N° 6683.<sup>23</sup> Sin embargo, el papel de los derechos de autor en la política de la ISP es problemático y debe abordarse de manera integral para que abarque el contenido de museos públicos, archivos, bibliotecas, galerías, etc.

**Costos e ingresos del gobierno.** El costo de la provisión de la información y los datos públicos no se presupuesta por separado, se incluye en los presupuestos regulares. Sin embargo, el gobierno es consciente de que es necesario definir políticas y brindar orientación en los casos en que las instituciones incurran en costos más altos para proveer la información solicitada. El gobierno no recibe ningún ingreso por la provisión de datos abiertos del gobierno.

**Tecnología, integridad y disponibilidad de los datos.** La información aún no está codificada, pero la codificación y la estandarización son parte de los Proyectos de Ley N° 19.113 y N° 20.361. Con respecto a la integridad, la información de planillas proviene directamente de INTEGRA y la información financiera de los sistemas de información del SIGAF del Ministerio de Hacienda, y la extracción de información directamente de estos sistemas garantiza la integridad.

El sitio web de Presidencia incluye una sección de Transparencia donde están disponibles gratuitamente los procedimientos, las Directrices ejecutivas y los informes presidenciales y generales. La administración planea publicar informes de viajes, planillas e informes de cesación de exfuncionarios.<sup>24</sup> Otras instituciones de importancia en materia de transparencia son:

- La **Contraloría General:** Sus proyectos incluyen: publicación de presupuestos institucionales y una plataforma informativa sobre recursos públicos llamada "*¿Sabes cómo se gasta tu dinero?*" La Contraloría participa en la Red Institucional de Transparencia que organiza la Defensoría de los Habitantes y en otras actividades de auditoría.
- La **Defensoría de los Habitantes:** Trabaja en transparencia, incluida la elaboración del Índice de Transparencia del Sector Público y el mantenimiento de la Red Institucional de Transparencia. El Proyecto de Ley N° 20.361 amplía sus responsabilidades.
- La **Dirección General del Archivo Nacional:** Promueve la digitalización de la información institucional.
- La **Procuraduría General:** Está principalmente a cargo de los principios éticos que deben ser respetados en el sector público.

**Interoperabilidad.** Actualmente no existen formatos estandarizados de publicación ni plataformas tecnológicas integradas para los sistemas de información y la entrega de información, pero están incluidos en los Proyectos de Ley N° 19.113 y N° 20.361. Está previsto establecer estándares que permitan la interoperabilidad de los sistemas de información entre las instituciones públicas y dentro de ellas, y que permitan que las tecnologías se utilicen de manera rentable, eficiente y segura.<sup>25</sup> El gobierno está considerando establecer parámetros generales para las plataformas que faciliten la inclusión de nuevas tecnologías de información.

**Digitalización de la ISP y el contenido.** La digitalización patrocinada por el gobierno será tomada en consideración al desarrollar las políticas.

### **Seguimiento y evaluación**

El Ministerio de Planificación Nacional y Política Económica (MIDEPLAN) es responsable de diseñar, dar seguimiento y evaluar el Plan Nacional de Desarrollo, incluido el Gobierno Abierto, utilizando un modelo de indicador-persona responsable-cronograma. Se presentan informes a MIDEPLAN semestralmente y a la Asociación de Gobierno Abierto anualmente. La ENGA ha desarrollado una matriz de evaluación e indicadores de implementación, seguimiento y evaluación de la transparencia y el acceso a la información pública, diseñados juntamente con la sociedad civil, la academia, la industria privada y las instituciones públicas. Todo esto está disponible en el sitio web de la Estrategia.<sup>26</sup> Se les da seguimiento a ocho proyectos de forma permanente:

1. La política de datos abiertos
2. El Decreto Ejecutivo sobre transparencia y acceso a la información pública
3. El progreso en los proyectos de ley sobre acceso a la información pública
4. El directorio de información sobre los perfiles de las instituciones públicas.
5. El diseño del plan piloto para la gestión de documentos y la administración de archivos
6. El fortalecimiento de la implementación y la aplicación de la Ley N° 8220 de Protección al ciudadano del exceso de requisitos y trámites administrativos.
7. El inventario y la promoción de plataformas tecnológicas para el desarrollo del Gobierno Abierto
8. El Índice de transparencia del sector público de la Defensoría de los Habitantes

A partir de la introducción de los Decretos Ejecutivos en 2017 el gobierno está trabajando con algunas instituciones para cumplir con el Índice de Transparencia de la Defensoría de los Habitantes, que contiene más de 150 indicadores.<sup>27</sup>

### **Datos e indicadores**

Los indicadores se centran en los datos de entrada más que en los de salida y en los indicadores clave de rendimiento. Los indicadores de entrada incluyen el cumplimiento de la estrategia, el seguimiento de la implementación, el porcentaje de realización y el monitoreo de la ejecución de las acciones. Los objetivos e indicadores de las políticas se definen y describen en el Eje de Transparencia y Acceso a la Información Pública de la ENGA.<sup>28</sup> La Defensoría de los Habitantes ha desarrollado e implementado el Índice de Transparencia del Sector Público, un indicador representativo y muy utilizado.<sup>29</sup> También está disponible la evaluación de la ENGA.<sup>30</sup>

### **Mejora de las políticas**

La matriz de evaluación de la ENGA permite mejorar los parámetros operativos, entre ellos:

- Ajuste de cronogramas
- Rendición de cuentas
- Asignación de responsabilidad
- Retroalimentación de los procesos

- Ejecución y optimización de propuestas

No hay datos disponibles sobre la ejecución de las mejoras y sobre los impactos de las mejoras de las políticas.

### 10.3. Valoración y recomendaciones

#### ***Recomendación del Consejo relativa al mejoramiento del acceso y un uso más eficaz de la información del sector público*** [[OCDE/LEGAL/0362](#)]

Costa Rica está planeando una política de información del sector público (ISP) a través de un Proyecto de Ley de Acceso a la Información Pública (Archivo N° 20.361) que permanece pendiente. Las dos líneas principales que enmarcan la política de ISP son la Estrategia de Gobierno Abierto y el libre acceso a datos abiertos, así como el contrapeso entre privacidad y protección de datos personales. Sin embargo, la información que abarca la Estrategia es más limitada que en la política integral de ISP, y se basa en el acceso a la información administrativa de interés público más que en la reutilización económica de toda la información y el contenido del sector público, la transparencia y la competencia justa. Hay un portal único de datos abiertos del gobierno, pero no está debidamente lleno, las normas son generales, es necesario aclarar el tratamiento de los derechos de autor, hay escasa evaluación de los efectos de la Estrategia y los indicadores de desempeño son principalmente indicadores de entrada. La política de ISP también carece de elementos tales como servidores públicos capacitados y una cultura institucional que facilite la disponibilidad de la ISP, así como presupuestos, herramientas tecnológicas y asociaciones público-privadas orientadas a desarrollar y aprovechar los datos públicos. Los esfuerzos de Gobierno Abierto son una solución parcial y el plazo para desarrollar la política de ISP sigue sin definirse; además, las regulaciones del acceso a la información aún son percibidas sectorialmente.

#### ***Recomendaciones***

- Desarrollar e implementar una política integral de ISP que abarque toda la información y el contenido del sector público y pueda aprovechar los beneficios económicos y sociales asociados.
- Implementar el portal único de datos del gobierno y alentar de manera proactiva a la administración, las instituciones autónomas y las empresas públicas a que lo llenen.
- Definir el papel de los derechos de autor, particularmente para abarcar el contenido de archivos públicos, bibliotecas, museos y galerías, y alentar a Costa Rica a considerar formas abiertas de derechos de autor y regímenes de propiedad intelectual similares a Creative Commons que faciliten la reutilización y hagan que las obras sean ampliamente accesibles y utilizables por parte del público.
- Fomentar una cultura de evaluación y supervisar las políticas y directrices de manera regular y coherente utilizando indicadores clave de rendimiento basados en resultados.

## 12. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) Y EL MEDIO AMBIENTE

### 11.1. Políticas

Costa Rica está planificando su primera política sobre TIC ecológicas. Costa Rica ha sido líder en TIC y medio ambiente en América Central, pero en este ámbito no ha definido una política pública específica. Sin embargo, iniciativas privadas como *Costa Rica verde e inteligente*, auspiciada por la Cámara Costarricense de Tecnologías de Información y Comunicación (CAMTIC) apoyan y fomentan el uso de tecnologías de la información favorables al medio ambiente.

En términos del desarrollo de políticas, en 2016 se creó la Comisión TIC y Medio Ambiente<sup>31</sup> como parte del Consejo Presidencial Social con dos tareas principales: colaborar en la ejecución de los objetivos medioambientales y de TIC del Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021,<sup>32</sup> y analizar y proponer una hoja de ruta nacional en esta materia. Dado que la política está en etapa de planificación, es muy pronto para delinear los futuros cambios en las políticas.

#### *Marco jurídico*

##### **Marco general de políticas**

Si bien Costa Rica no cuenta con una política específica en materia de las TIC y el medio ambiente, sí existe un marco regulatorio integral de políticas generales. De conformidad con el artículo 129 de la Constitución Política las obligaciones en materia ambiental y TIC son vinculantes, y la Ley N° 6227, Ley General de la Administración Pública, establece la jerarquía de todas las normas y reglamentos. El marco regulatorio está definido por los reglamentos y otros actos escritos o no escritos que emiten los órganos públicos pertinentes.

Los objetivos del PNDT relacionados con el Plan Nacional de Energía y de Ambiente, así como el propio PNDT, son vinculantes a nivel presupuestario, de conformidad con el artículo 4 de la Ley de la Administración Financiera de la República y Presupuestos Públicos (N° 8131).

Conforme a los artículos 2 y 4 del Decreto Ejecutivo N° 38536-MP-PLAN, Reglamento Orgánico del Poder Ejecutivo, al Ministro de Ambiente y Energía se le asigna la función de Rectoría del medio ambiente. El reglamento otorga autoridad al Presidente de la República, juntamente con la o el Ministro Rector para coordinar, articular y conducir las actividades de cada sector conforme a las orientaciones del Plan Nacional de Desarrollo (PND), y para coordinar, dar seguimiento y evaluar los resultados de las actividades que realicen las instituciones de cada sector para ejecutar las políticas públicas sectoriales, regionales e institucionales. En determinadas materias de especial interés para el Estado, la rectoría del Poder Ejecutivo puede extenderse al ámbito privado.

Finalmente, las sentencias, los votos y la jurisprudencia de la Sala Constitucional de la Corte Suprema de Justicia son vinculantes *erga omnes* (para todos), de acuerdo con el Artículo 13 de la Ley de la Jurisdicción Constitucional (N° 7135), conforme a su Sentencia N° 3309-94 del 5 de julio de 1994, que declara: "(...) la reforma (del artículo 188 de la Constitución Política) hizo constitucionalmente posible someter a las entidades autónomas en general a los criterios de planificación nacional y en particular, someterlas a las directrices de carácter general dictadas desde el Poder Ejecutivo central o de órganos de la Administración Central."

##### **Marcos políticos y jurídicos detallados**

Actualmente existen marcos regulatorios y jurídicos detallados que son pertinentes para las TIC y el medio ambiente; el PNMT, por ejemplo, incluye objetivos específicos cuyo cumplimiento implica que los ministerios emprendan proyectos relacionados con la innovación y las TIC en beneficio del medio ambiente (ver más adelante).

La Ley para la Gestión Integral de Residuos (N° 8839) del 13 de julio de 2010 estableció el principio de "responsabilidad extendida del productor". Los productores o importadores son responsables del producto a lo largo de su ciclo de vida, incluidas las fases posindustriales y posconsumo. Este principio solo se aplica a los desechos que requieren un manejo especial, incluidos los electrónicos.<sup>33</sup>

Las instituciones estatales tienen varios mecanismos para poner a disposición la información ambiental del país. En concreto, se creó el Sistema Nacional de Información Ambiental (SINIA) bajo la responsabilidad del Centro Nacional de Información Geoambiental (CENIGA) y el Ministerio de Ambiente y Energía (MINAE). El CENIGA había identificado que se requerían capacidades institucionales mejoradas para optimizar los flujos de información. El artículo 1 declara: "...El Sistema Nacional de Información Ambiental se constituye en la plataforma oficial de coordinación y vinculación institucional y sectorial del Estado costarricense para facilitar la gestión y distribución del conocimiento de la información ambiental nacional."<sup>34</sup>

En otras áreas, las políticas relacionadas con las TIC y el medio ambiente incluyen:

- **Política de energía.** El Plan Nacional de Energía 2015-2030 incluye elementos relacionados con las TIC.<sup>35</sup> El Plan incluye un suministro de energía de bajas emisiones que respeta el desarrollo sostenible y equilibra los objetivos económicos, ambientales y sociales; y abarca, entre otros aspectos, directrices para que el sector del transporte promueva un transporte público eficiente y más limpio, fomente el uso de combustibles alternativos y mejore los estándares de consumo de energía y contaminación en los vehículos importados nuevos y usados. Un ejemplo específico incluye el fortalecimiento de la Red Nacional de Monitoreo de la Calidad del Aire y un mejor uso de los datos con el fin de mejorar las políticas públicas (Objetivo 5.1), así como el uso de tecnologías para reducir los impactos ambientales de la flota de vehículos públicos (Objetivo 5.2).
- **Política ambiental.** Costa Rica tiene políticas que fomentan el uso de tecnologías digitales de bajo impacto ambiental. Esto incluye regulaciones para promover el uso de recursos compartidos y servicios en la nube (MICITT, Directriz N° 046-H-MICITT).

### ***Responsabilidades y facultades***

Como se describe en la sección 11.1, las políticas en materia de TIC y medio ambiente están en su etapa inicial en Costa Rica, pero se prevé que la Comisión TIC y Medio Ambiente, compuesta por múltiples partes interesadas, impulsará y dará seguimiento a este tipo de políticas. El gobierno planea desarrollar un entendimiento común sobre temas que incluyen: el efecto directo de las TIC en el medio ambiente; el potencial y los beneficios de las TIC en el sector ambiental; y el potencial y los beneficios de las TIC para cambiar el comportamiento social y cultural relacionado con el medio ambiente.<sup>36</sup> Durante el desarrollo de la política se decidirán las funciones relacionadas con la implementación, evaluación y cumplimiento de las políticas de TIC y medio ambiente y la función de las partes interesadas no gubernamentales, el sector empresarial y la sociedad civil.

El Plan Nacional de Desarrollo de las Telecomunicaciones incluye el objetivo específico de que los 18 Ministerios tengan un proyecto de innovación y uso de TIC en beneficio del medio ambiente y que el MICITT lo supervise. Cada ministerio debe definir y desarrollar los proyectos que se adapten mejor a sus necesidades.

### ***1 – Coordinación de las políticas de TIC, clima, medio ambiente y energía***

La política es impulsada y supervisada por la Comisión TIC y Medio Ambiente que, aunque es interinstitucional, la lidera el Poder Ejecutivo. El Ministerio de Ambiente y Energía, como Rector responsable de la coordinación del desarrollo de las políticas, garantiza la coherencia de las políticas, aunque las decisiones se toman por consenso.

El Ministro de Ambiente y Energía emite reglamentos, directrices, circulares y otros actos internos para el Ministerio y para otras entidades públicas en los ámbitos de medio ambiente y energía. Las disposiciones del artículo 28 de la Ley General de la Administración Pública (N° 6227) y los artículos 2 y 4 del Decreto Ejecutivo N° 38536-MP-PLAN, Reglamento Orgánico del Poder Ejecutivo, les otorgan poder al Presidente y al Ministro Rector para coordinar y realizar actividades conjuntas en cada sector.

El artículo 2 de la Ley Orgánica del Ministerio de Ambiente y Energía (N° 7152) le asigna a este Ministerio las funciones de formular, planificar y ejecutar las políticas de recursos naturales, energéticas, mineras y de protección ambiental, así como de la dirección, el control, la fiscalización, la promoción y el desarrollo en estos campos. El MINAE también debe realizar y supervisar las investigaciones, las exploraciones técnicas y los estudios económicos de los recursos del sector.

### ***2 – Adopción de perspectivas del ciclo de vida***

La Ley para la Gestión Integral de Residuos (N° 8839) regula los residuos y su ciclo de vida. Esta Ley dispone un conjunto detallado e interrelacionado de acciones regulatorias, operativas, financieras, administrativas, educativas, de planificación y de monitoreo y evaluación para la gestión de residuos desde su generación hasta su disposición final. En el caso de los residuos electrónicos, el Decreto Ejecutivo N° 35933-S, Reglamento para la Gestión Integral de los Residuos Electrónicos, establece mecanismos para que los usuarios, productores y gerentes trabajen de manera articulada una vez que los equipos se consideren residuos.<sup>38</sup>

El Reglamento también creó el Sistema Nacional para la Gestión Integral de los Residuos Electrónicos (SINAGIRE) y el Comité Ejecutivo para la Gestión Integral de los Residuos Electrónicos (CEGIRE). El CEGIRE implementa buenas prácticas y el concepto del ciclo de vida de las TIC en procura de mejoras ambientales. El CEGIRE y el Ministerio de Salud están coordinando el desarrollo y la implementación de un sistema de información para cuantificar la recolección y la gestión de residuos electrónicos, actividades de reciclaje, etc., pero aún no existen datos sobre cantidades e impactos.

### ***3 – Apoyo a la investigación e innovación en tecnologías y servicios ecológicos***

El MICITT no tiene programas dedicados a investigaciones de largo plazo en tecnologías y servicios verdes. Sin embargo, los últimos dos Planes Nacionales de Ciencia y Tecnología han incluido convocatorias anuales de investigación en estos temas. Por ejemplo, la convocatoria de 2016 incluyó fondos para el desarrollo de energías renovables, y el Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021 incluye el desarrollo tecnológico de una red eléctrica inteligente, tecnologías de almacenamiento de energía a gran escala, investigación relacionada con la dinámica del transporte y el desarrollo de combustibles alternativos, y el uso eficiente de la biomasa y el hidrógeno. El MICITT también ha brindado apoyo financiero a proyectos de investigación como el "Atlas de la Biodiversidad de Costa Rica" y a la mejora de los procesos agrícolas y el uso sostenible del agua (véase la Recomendación 9 más adelante).

La principal empresa pública de energía, el Instituto Costarricense de Electricidad, tiene un Laboratorio de Eficiencia Energética<sup>39</sup> y programas de investigación en biocombustibles,<sup>40</sup> energía solar y fuentes de energía alternativa. El CIVCO, un centro de investigación del Instituto Tecnológico de Costa Rica ha realizado investigaciones en tecnologías ecológicas para la construcción desde 2001 y cuenta con diferentes programas y patentes.<sup>41</sup> El Plan

Nacional de Energía 2015–2030 incluye I+D en energías renovables no convencionales bajo el objetivo estratégico 7.3: "Diversificar la matriz energética".

En 2015 Costa Rica aprobó por decreto una Política Nacional de Compras Públicas Sustentables cuyo objetivo principal es propiciar la estimulación de la producción de bienes y servicios con innovación y el mejor desempeño económico, ambiental y socialmente responsable. Esta norma se encuentra en sus primeras etapas e incluye la investigación y la creación de una Comisión Nacional con representantes de alto nivel.<sup>42</sup>

La Comisión TIC y Medio Ambiente también apoyará la investigación ambiental en, por ejemplo, universidades.

#### ***4 – Desarrollo de habilidades en TIC ecológicas***

El sistema educativo de Costa Rica favorece la educación técnica y la capacitación como respuesta a las demandas del sector productivo. Este sistema fomenta el desarrollo de habilidades, ya sea en un puesto de trabajo o entre personas desempleadas con el objetivo de su reinserción en el mercado laboral. Se están desarrollando mecanismos que le permitan al personal técnico de las municipalidades desarrollar habilidades en tecnologías verdes y, en general, como parte de la política implementada a través de las universidades y el Instituto Nacional de Aprendizaje (INA).

La educación de los técnicos se realiza a través del Ministerio de Educación Pública (MEP) o del INA. La Educación Vocacional Técnica del MEP incluye capacitación teórica y práctica en un campo técnico que culmina con la obtención de un diploma de técnico de nivel medio. El INA y, en menor medida, empresas y organizaciones privadas, imparten capacitación técnica para técnicos especializados.

En 2007 el MEP creó la Dirección de Recursos Tecnológicos en Educación (DRTE), a cargo de supervisar la introducción o el uso de las TIC en el sistema educativo; y las TIC están incluidas en los planes de estudio nacionales como parte de los Objetivos Estratégicos Institucionales del MEP, 2015-2018. También se ha desarrollado el Programa Nacional de Tecnologías Móviles "Tecno@prender" (PNTM) de la DRTE como apoyo de los objetivos educativos a través de la tecnología móvil.

El INA tiene una política ambiental aprobada por la Junta Directiva el 20 de septiembre de 2010 (Resolución N° 143-2010-JD, modificada el 16 de enero de 2012 mediante la Resolución N° 004-2012-JD). El INA, en cumplimiento del objetivo 6 de su Plan Estratégico Institucional (PEI) y como parte de los pasos necesarios para convertirse en una institución sostenible, tiene la meta de obtener la certificación ISO 14001 de su Sistema de Gestión Ambiental (SGA), tanto en apoyo administrativo y de gestión como en los Servicios de Educación y Formación Profesional (SEFP).<sup>43</sup>

Para implementar el SGA, el INA ha conformado 17 Subcomités Ambientales que abarcan los 12 Núcleos de Servicios de Capacitación Tecnológica, nueve Unidades Regionales y 54 Centros de Capacitación, ha elaborado documentos y procedimientos en el Sistema de Información de Calidad y ha definido los siguientes compromisos ambientales:

- **Gestión del aire (cambio climático):** Sensibilizar a la población del INA en temas de contaminación del aire, neutralidad en emisiones de carbono y el inventario de emisiones institucionales.
- **Gestión del agua:** Uso responsable de los recursos hídricos y gestión de residuos líquidos.
- **Gestión del suelo y residuos sólidos:** Fomentar la separación y el tratamiento de los residuos sólidos.
- **Gestión de la energía:** Uso responsable de la energía y las tecnologías que reducen el consumo de electricidad.

- **Adquisición de bienes (compras sustentables):** Análisis e inclusión de criterios ambientales en la adquisición de bienes institucionales.

Con la implementación del SGA, el uso de recursos en las instalaciones del INA se redujo en un 1-5% en 2015.<sup>44</sup> En 2016 se produjeron reducciones de 3.3% en combustible para transporte, de 6% en gasolina y 69% en acetileno para usos fijos, compensados por aumentos significativos en el consumo de diésel y gas LPG para usos fijos (65% y 75%, respectivamente). El consumo de electricidad, agua y papel se redujo en 0.3%, 9% y 12% respectivamente. El INA también implementó un Sistema de Información de Indicadores Ambientales para cumplir con las regulaciones en materia de desarrollo de programas institucionales de gestión ambiental y respaldar la certificación ISO 14001.

Por último, desde 2010 el INA ha emitido directrices sobre el diseño y desarrollo de SEFP que obligan a las unidades estratégicas a incorporar empleos verdes y sostenibilidad ambiental como piedras angulares en todas las evaluaciones, el diseño y los ajustes de las necesidades del mercado laboral. En 2016 se graduaron 11 192 personas en ocupaciones relacionadas con las TIC, pero no se recopiló cifras específicamente relacionadas con las TIC verdes.

### *5 – Aumentar la conciencia pública sobre el papel de las TIC en la mejora del desempeño ambiental y 6 – Fomentar las mejores prácticas)*

Costa Rica está desarrollando una política pública en materia de TIC y el medio ambiente basada en tres pilares. El primero se centra en la promoción de la investigación y se lleva a cabo en colaboración con la comunidad académica. El segundo se centra en el fortalecimiento de las capacidades y se lleva a cabo en colaboración con el Instituto Nacional de Aprendizaje (INA). El tercero se basa en información dirigida al público general y a las personas consumidoras sobre el uso de la tecnología y su potencial para mejorar el desempeño ambiental, y está siendo llevado a cabo por el MICITT, el MINAE, las municipalidades y otros actores. Conforme al PNDDT, los 18 ministerios deben implementar un proyecto de uso e innovación de TIC beneficiosas para el medio ambiente.

Costa Rica también ha promovido una cultura de desarrollo sostenible en la legislación, las empresas y el comportamiento ciudadano. Uno de los mecanismos ha sido la creación de programas voluntarios para empresas e instituciones que procuran mejorar su desempeño ambiental. Estos programas incluyen:

2. **Programa país de carbono neutralidad.** A junio de 2017 había 85 instituciones certificadas por este programa.
3. **Sistema de Reconocimientos Ambientales.** Reconoce a las organizaciones que han provocado un cambio significativo en el campo ambiental nacional que contribuye a alcanzar los objetivos del Plan Nacional de Desarrollo y del desarrollo sostenible a largo plazo; abarca cuatro áreas: producción limpia, ecoeficiencia, responsabilidad social y emprendimientos ambientales.
4. **Programa de Bandera Azul Ecológica.** Alienta a los comités locales a promover la eficiencia de los recursos y reducir impactos ambientales negativos como las emisiones de GEI. En 2016 se inscribieron 4976 Comités Locales y 3051 (61.3%) obtuvieron la Bandera Azul.
5. **Certificado de Sostenibilidad Turística.** Se otorgado en seis categorías: hoteles, operadores turísticos, restaurantes, parques temáticos, alquiler de autos y operadores turísticos marinos. A mayo de 2017 se había certificado a 370 organizaciones turísticas.

Costa Rica también ha ordenado que todas las instituciones del sector público implementen el Programa de Gestión Ambiental Institucional (PGAI) para fomentar un enfoque integrado de gestión de residuos, el uso eficiente de los recursos energéticos y el uso de tecnologías más limpias en la Administración Pública (véase más adelante la Recomendación 7 - Gobiernos que lideran con el ejemplo).

En 2016 el MICITT otorgó becas a estudiantes y profesores universitarios costarricenses para que asistieran al Foro Mundial de Tecnología de Información (WITFOR 2016) en San José, iniciado por la Federación Internacional para el Procesamiento de la Información ([www.witfor2016.org](http://www.witfor2016.org)) Reunió a representantes de gobiernos, la academia, industria y asociaciones para discutir propuestas para alcanzar los objetivos de desarrollo sostenible de la ONU y mejorar las condiciones mundiales: reducción de la pobreza y el hambre; educación universal; promoción de la igualdad de género; asegurar la sostenibilidad ambiental; y la lucha contra enfermedades y la reducción de la mortalidad.

El MICITT también está desarrollando campañas para sensibilizar sobre la importancia de gestionar los residuos electrónicos como parte de la migración de la televisión analógica a la digital.

### ***7 – Gobiernos que lideran con el ejemplo***

El gobierno ha venido tomando acciones concretas en temas ambientales. El sector público ha implementado el Programa de Gestión Ambiental Institucional (PGAI) que establece el Decreto Ejecutivo N° 36499-S-MINAET (seguido por las municipalidades conforme al artículo 28 de la Ley N° 8839), así como el Reglamento para la Elaboración de Programas de Gestión Ambiental Institucional en el Sector Público de Costa Rica.<sup>45</sup> Específicamente, el reglamento se ajusta al requisito del artículo 28 de la Ley para la Gestión Integral de Residuos (N° 8839), que describe la responsabilidad de crear sistemas de gestión ambiental en instituciones, empresas públicas y municipalidades. (Véase *Marcos políticos y jurídicos detallados* y la Recomendación 2).

Costa Rica ha promovido el teletrabajo en tres decretos ejecutivos y planes de acción, y las instituciones públicas tienen la instrucción de tener en cuenta tecnologías favorables con el medio ambiente como los servicios en la nube. El resultado es que en el sector público la adopción del teletrabajo es mayor que en las empresas privadas:<sup>46</sup>

- el 29.7% de las instituciones públicas aplicaron teletrabajo en agosto de 2016.
- En las instituciones que aplican teletrabajo, el 53% de los teletrabajadores están en puestos profesionales, un 18% en puestos administrativos y otro tanto en puestos técnicos, y el 11% en la sede central.
- En marzo de 2017 aproximadamente 2500 empleados públicos teletrabajaron.
- El teletrabajo se realiza con mayor frecuencia durante dos o tres días a la semana.

Una encuesta realizada por "Business pulse" en el cuarto trimestre de 2016 mostró que solo el 21% de las 400 empresas privadas entrevistadas aplicaban teletrabajo.

### ***8 – Mejora de la contratación pública***

Los aspectos ambientales tienen un papel importante en la contratación pública. Las adquisiciones y contrataciones del sector público están reguladas por el Decreto Ejecutivo N° 39310-H-MINAE-MEIC-MTSS de los Ministerios de Hacienda, de Ambiente y Energía (MINAE), de Economía, Industria y Comercio (MEIC) y de Trabajo y Seguridad Social (MTSS).<sup>47</sup> Este decreto apunta a estimular, a través del poder adquisitivo del Estado, la producción de bienes y servicios innovadores y mejorados en materia ambiental y socialmente responsables. El Ministerio de Hacienda y el MICITT también presentaron la Directriz Pública N° 046-H-MICITT relativa a la importancia de las TIC y el trabajo del Estado en su implementación, con base en los principios del uso eficiente de los recursos y una implementación más eficaz.

Al evaluar las licitaciones y las contrataciones directas, los Ministerios deben añadir un 20% de valoración a los productos que incorporen criterios de gestión integral de residuos en su ciclo de vida útil.<sup>48</sup> En el caso de la gestión de residuos electrónicos, véase también la sección *11.1 Marco jurídico*, la Recomendación 2 – Adopción de perspectivas del ciclo de vida, y la Recomendación 7 – Gobiernos que lideran con el ejemplo. Sobre el

Reglamento para la Elaboración de Programas de Gestión Ambiental Institucional, véase la Recomendación 7 – Gobiernos que lideran con el ejemplo.

### **9 – Fomento de la medición**

El gobierno fomenta el desarrollo de aplicaciones de TIC para medir y monitorear los desafíos ambientales en organizaciones gubernamentales y no gubernamentales. El MICITT aporta apoyo financiero a proyectos de investigación como el "Atlas de la Biodiversidad de Costa Rica" (CRBio 2.0). El sitio web asociado ([www.crbio.cr](http://www.crbio.cr)) provee acceso gratuito a información sobre la biodiversidad de Costa Rica y las investigaciones relacionadas con ella, educación y desarrollo sostenible. La base de datos comprende más de seis millones de registros de especímenes recolectados u observados en Costa Rica por científicos de 169 instituciones y 34 países. El sitio utiliza y adapta software gratuito desarrollado por Atlas of Living Australia y la Infraestructura Mundial de Información en Biodiversidad (GBIF por sus siglas en inglés, [www.gbif.org](http://www.gbif.org)).

La GBIF, la iniciativa en informática de la biodiversidad más importante del mundo es el resultado de una recomendación de 1999 del Subgrupo de Informática de la Biodiversidad del Foro de Megaciencia de la OCDE. Costa Rica es miembro fundador desde 2001 y CRBio se creó inicialmente como el nodo de la GBIF en Costa Rica. Con el liderazgo de INBio (Instituto Nacional de Biodiversidad), Costa Rica ha desempeñado un papel muy activo en la GBIF a nivel científico, técnico y de desarrollo de capacidades. El director de la delegación costarricense presidió el Comité Científico de la GBIF entre 2007 y 2009 y presidió el Subcomité de Extensión y Desarrollo de Capacidades entre 2001 y 2005. Además, los miembros de la delegación costarricense lideran programas de mentoría patrocinados por la GBIF para establecer plataformas de TIC de biodiversidad en Perú, Nicaragua, Argentina, Benín y Chile.

Por último, el MICITT tiene un programa permanente de innovación con el sector productivo para difundir las mejores prácticas, incluso en relación con TIC. El trabajo realizado para mejorar los procesos agrícolas y el uso sostenible del agua son buenos ejemplos del uso de las TIC para enfrentar los desafíos de monitoreo y gestión de los recursos naturales.

En términos de medición y monitoreo con TIC, Costa Rica ha establecido el marco institucional y está consolidando el Sistema Nacional de Información Ambiental (SINIA) de conformidad con el Sistema Estadístico Nacional. El SINIA recibe información ambiental de sistemas establecidos para temas específicos.

### **11.3. Seguimiento y evaluación**

El proceso para crear una política de TIC verdes ha comenzado y el gobierno está recopilando información y revisando las políticas ambientales nacionales para facilitar este proceso.

#### **10 - Establecer objetivos de política y aumentar la evaluación**

Dado que Costa Rica aún no tiene una política de TIC verdes, todavía no se han desarrollado datos e indicadores para medir la efectividad de la política. No se han proporcionado datos sobre la efectividad de varias subáreas de políticas; por ejemplo, la aplicación del reglamento de gestión de residuos electrónicos (Recomendación 2), o los resultados de la educación y capacitación en TIC verdes (Recomendación 4).

Costa Rica ha establecido el marco institucional y está consolidando el Sistema Nacional de Información Ambiental (véase la Recomendación 9). No obstante, el país debe mejorar sus capacidades para generar una gama más amplia de indicadores de alta calidad para medir el desempeño de las políticas ambientales. Con este fin, el gobierno está trabajando en la modernización de las plataformas de comunicación del sistema y publicará el primer

Informe sobre el Estado del Medio Ambiente para sensibilizar y facilitar el uso de la información ambiental en la adopción de decisiones.

#### 11.4. Valoración y recomendaciones

##### ***Recomendación del Consejo relativa a las tecnologías de información y comunicación y el medio ambiente [OECD/LEGAL/0380]***

Costa Rica no tiene una política específica en materia de tecnologías de información y comunicación (TIC) verdes, pero tiene una serie de acciones y planes relacionados con la Recomendación que reflejan el papel proactivo y altamente desarrollado del gobierno de Costa Rica en la protección del medio ambiente y la biodiversidad. Se está desarrollando una política general sobre las TIC y el medio ambiente, se han implementado algunos elementos y algunas acciones específicas abarcan aspectos de las recomendaciones 1-8 de la Recomendación. Sin embargo, solo hay datos limitados, o inexistentes, sobre la medida en que se han adoptado los enfoques del ciclo de vida, el éxito del reciclaje de residuos electrónicos y la medida en que se han desarrollado empleos y ocupaciones verdes y capacitación en ellos. Por otra parte, podría llevarse a cabo un uso más específico de las TIC y enfoques concertados para difundir información sobre las mejores prácticas y sus beneficios, así como reconocer más explícitamente los potenciales beneficios ambientales.

##### ***Recomendaciones***

- Desarrollar una política integral para las TIC y el medio ambiente a partir de los marcos ya existentes.
- Ampliar las iniciativas gubernamentales existentes para mejorar la conciencia pública sobre el papel de las TIC en la mejora del desempeño ambiental y fomentar una difusión más extendida de las mejores prácticas en materia de TIC y medio ambiente.
- Desarrollar indicadores clave y recopilar datos para monitorear y evaluar las interacciones entre las TIC y el medio ambiente y que incluyan áreas clave como el teletrabajo, la contratación pública, la gestión de residuos, la capacitación y las habilidades.

## 12. PRIVACIDAD

### 12.1. Políticas

El objetivo de la política de privacidad de Costa Rica es garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Costa Rica procura equilibrar su visión de un sistema flexible y eficiente que le permita al país ser competitivo en la era de los macrodatos y al mismo tiempo proteger los datos personales.

#### *Marco jurídico*

La Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (N° 8968) de 2011 establece el principal marco legislativo para la protección de datos personales en Costa Rica. Su objetivo es garantizar el respeto del derecho fundamental de las personas a la autodeterminación informativa, es decir, el derecho de controlar el flujo de información sobre cada persona e impedir la discriminación. La Ley N° 8968 establece el régimen general de protección de datos en Costa Rica y abarca el procesamiento automatizado o manual de datos personales por parte de entes públicos o privados en el país y a cualquier tipo de uso posterior de estos datos. Crea un registro nacional de las bases de datos que operan en el país; define los derechos de los interesados y establece mecanismos de protección; contiene restricciones para el procesamiento de datos confidenciales; dispone un conjunto de obligaciones para los controladores y procesadores de datos; y establece un conjunto de principios principales: legalidad, limitación de propósito, consentimiento, calidad de los datos, transparencia, acceso limitado, seguridad, confidencialidad.

La Ley N° 8968 estableció la Agencia de Protección de Datos de los Habitantes (PRODHAB) como el órgano principal a cargo de la aplicación de la ley de protección de datos personales de Costa Rica. La Agencia debe mantener una lista de bases de datos reguladas y toda la información necesaria para hacer cumplir eficazmente las normas de protección de datos personales; resolver reclamaciones de violaciones de la normativa de protección de datos personales y ordenar que se eliminen, rectifiquen, completen o modifiquen los datos que violen las normas; imponer sanciones; contribuir al desarrollo de regulaciones en materia de protección de datos personales; desarrollar las instrucciones necesarias para las instituciones públicas; y concientizar a los habitantes sobre sus derechos con respecto al procesamiento de sus datos personales.

En 2012 Costa Rica promulgó el primer Reglamento de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales fue creado mediante el Decreto Ejecutivo 37554-JP y está en vigor desde 2013. En diciembre de 2016, el Decreto Ejecutivo N° 40008-JP reformó el Reglamento para aclarar el texto y simplificar los procedimientos. La Ley N° 8968 sobre cómo actuar en relación con el procesamiento de datos personales ha estado en vigor desde 2014.

- **Principio de limitación de la recolección:** El artículo 4 de la Ley N° 8968 establece el derecho a la autodeterminación informativa, que les permite a todas las personas controlar el flujo de informaciones sobre su persona. El Artículo 5 establece el Principio de consentimiento informado, según el cual los datos solo pueden procesarse si se cuenta con consentimiento informado previo y por escrito. El consentimiento puede ser revocado de la misma manera.
- **Principio de calidad de la información:** El artículo 6 de la Ley N° 8968 contiene el Principio de calidad de la información, que establece que los datos

personales solo pueden ser recolectados, almacenados o empleados cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.

- **Propósito especificación del propósito:** El artículo 5.1 b de la Ley N° 8968 especifica que, cuando se solicita información personal, es obligatorio informar a la persona de los propósitos de la recolección de datos personales de manera expresa, precisa e inequívoca.
- **Principio de limitación del uso:** El artículo 5.2 de la Ley N° 8968 (concerniente al otorgamiento del consentimiento) establece que el procesador de datos debe obtener el consentimiento expreso de la persona titular de los datos. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, y puede ser revocado de la misma manera, sin efecto retroactivo. No se requiere el consentimiento expreso cuando: exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo; se trate de datos obtenidos de fuentes de acceso público genera; y los datos deban ser entregados por disposición constitucional o legal.
- **Principio de salvaguardas de la seguridad:** El artículo 10 de la Ley N° 8968 establece que el responsable de los datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado.
- **Principio de apertura:** El artículo 12 de la Ley N° 8968 establece que los procesadores de datos (personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales), podrán emitir y registrar ante la PRODHAB protocolos en los que establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley.
- **Principio de participación individual:** El artículo 7 de la Ley N° 8968 garantiza el derecho de toda persona al acceso de sus datos personales sin demora y de forma gratuita y a obtener la rectificación y actualización o supresión de sus datos personales cuando hayan sido tratados en violación de las disposiciones de la Ley N° 8968. La rectificación, actualización o supresión de datos personales debe realizarse en el plazo de los cinco días hábiles siguientes a la recepción de la solicitud por parte de la persona responsable de la base de datos. El artículo 13 prevé que las personas también pueden utilizar un procedimiento administrativo sencillo y rápido ante la PRODHAB para solicitar protección contra actos que violen sus derechos fundamentales. La PRODHAB puede ordenar, de oficio o ante solicitud de una parte, que los datos sean suprimidos, rectificados, completados o modificados cuando infrinjan las normas de protección de los datos personales.
- **Principio de responsabilidad:** El artículo 31 del Decreto Ejecutivo N° 37554-JP establece las obligaciones de las personas responsables del tratamiento de datos personales. La Ley N° 8968 prevé un procedimiento sancionatorio.
- **Parte tres, Implementación de la responsabilidad:** El artículo 12 de la Ley N° 8968 y al artículo 32 del Decreto Ejecutivo N° 37554-JP establecen que las personas que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales deben emitir un programa de gestión de la privacidad o “protocolo” que defina las reglas para la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con la Ley N° 8968.

- **Principios básicos de aplicación internacional: Flujo libre y restricciones legítimas:** Costa Rica no restringe los flujos transfronterizos de datos personales, excepto en el caso de datos sensibles.
- **Implementación nacional:** La Ley N° 8968 protege la privacidad, establece la PRODHAB como autoridad de fiscalización de la privacidad, dispone medios razonables para que las personas ejerzan sus derechos, sanciona el incumplimiento de las leyes que protegen la privacidad, incluye educación y sensibilización, asegura que no haya discriminación injusta contra las personas titulares de los datos y toma en consideración la función de los actores relevantes.
- **Cooperación internacional:** Costa Rica ha comenzado a adoptar medidas para facilitar la cooperación transfronteriza para la aplicación de las leyes de privacidad y para establecer procedimientos para la cooperación internacional.

### *Responsabilidades y facultades*

La PRODHAB tiene plena responsabilidad y autoridad para desarrollar políticas nacionales de privacidad y garantizar el cumplimiento de las normas sobre protección de datos. La PRODHAB es una agencia independiente del Ministerio de Justicia y Paz cuyas responsabilidades incluyen el registro y el acceso a bases de datos, la resolución de reclamaciones, la imposición de sanciones por violaciones de las normas de protección de datos personales, y la emisión de directrices para las instituciones públicas sobre cómo manejar los datos personales (el Recuadro 12.1 incluye una descripción completa).

#### **Recuadro 12.1. Atribuciones de la PRODHAB (según el Artículo 16 de la Ley N.º 8968)**

- Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
- Llevar un registro de las bases de datos reguladas por esta ley, con las informaciones necesarias provistas por quienes administren las bases de datos.
- Acceder a las bases de datos reguladas, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales.
- Resolver los reclamos por infracción a las normas de protección de los datos personales.
- Ordenar la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.
- Imponer las sanciones establecidas a las personas físicas o jurídicas que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito.
- Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.
- Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales.
- Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

La PRODHAB puede imponer las siguientes penas por violaciones de las normas de protección de datos personales: por delitos menores, multas de hasta cinco veces el salario base mensual<sup>49</sup>; por delitos graves, de cinco a veinte veces el salario base mensual; y para delitos muy graves, de quince a treinta veces el salario base mensual y 6 meses de suspensión de la operación de la base de datos.

Además, cabe señalar que el Poder Judicial tiene un grupo especializado llamado Sección de Delitos Informáticos que lleva a cabo investigaciones sobre cuestiones relativas ciberdelincuencia, incluidas las relacionadas con la protección de datos.

Las partes interesadas no gubernamentales, en particular las empresas, la academia y la sociedad civil desempeñan una función importante en la formulación de políticas en Costa Rica. En particular, la PRODHAB fomenta la participación de sectores técnicos especializados en el desarrollo de nueva normativa. Cada acto legislativo está sujeto a un período de consulta pública y los comentarios deben tomarse en consideración antes de su promulgación. Por otra parte, las partes interesadas no gubernamentales pueden promover o solicitar normas o estándares no reglamentarios en materia de privacidad y protección de datos; por ejemplo, por parte del Instituto de Normas Técnicas de Costa Rica (INTECO) y otras entidades similares.

## 12.2. Implementación

La PRODHAB está desarrollando una metodología para hacer cumplir plenamente la ley sobre datos personales, realizar intervenciones y auditar su uso. La metodología se publicará en el Plan Estratégico de la Agencia, cuya publicación está prevista para finales de 2017. Este plan incluirá las metas, los objetivos y el plan de trabajo para los próximos cinco años. Además, la Agencia ha continuado capacitando a entidades públicas, funcionarios públicos y ciudadanos y ha lanzado un plan de comunicación en esta primera mitad de 2017.

### *Medidas no regulatorias*

La PRODHAB considera esencial la educación de las empresas y los usuarios en el desarrollo de una cultura de privacidad. La Agencia concientiza a los ciudadanos y empresas acerca de sus derechos y responsabilidades en relación con el acopio, el almacenamiento, la transferencia y el uso de sus datos personales. La Agencia capacita a entidades públicas, funcionarios públicos y ciudadanos a través de charlas y conferencias, entre otros medios. En 2016 la Agencia se centró en educar y ayudar a los gobiernos locales. En 2017 el objetivo es desarrollar la cooperación con la agencia de protección al consumidor y la Defensoría de los Habitantes. La PRODHAB lanzó un plan mediático en el primer semestre de 2017 con el fin de crear conciencia sobre la protección de datos y la privacidad. Estas actividades cuentan con el respaldo del sector empresarial y las instituciones públicas.

### *Aplicación de la ley*

La política de privacidad y protección de datos es aplicada judicialmente y por la PRODHAB, encargada de resolver los reclamos por violación de las normas de protección de datos personales y de salvaguardar los derechos de las personas (artículo 24). La PRODHAB también puede dictar medidas cautelares (artículo 25) e imponer sanciones (artículo 28 )

Entre mediados de 2014 y principios de 2017, la PRODHAB procesó 150 casos presentados por ciudadanos en relación con el uso inapropiado de datos personales en una amplia gama de situaciones, como productos financieros, hospitales o loterías. La mayoría de las reclamaciones se refirió a productos financieros.

La PRODHAB está desarrollando una metodología para hacer cumplir plenamente la ley sobre datos personales, realizar intervenciones y auditar su uso. Está prevista la publicación

de la metodología en el Plan Estratégico de la Agencia a finales de 2017. El plan incluirá las metas, los objetivos y el plan de trabajo para los próximos cinco años.

### ***Cooperación transfronteriza***

Con respecto a la cooperación transfronteriza para la aplicación de las leyes de privacidad y protección de datos, la PRODHAB es miembro de la Red Iberoamericana de Protección de Datos y participa en conferencias internacionales de privacidad. Costa Rica planea adoptar medidas para firmar el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, y también está interesada en unirse a la Red Global de Vigilancia de la Privacidad (GPEN por sus siglas en inglés).

Costa Rica también ratificó recientemente la "Convención sobre Ciberdelincuencia" (conocida como la Convención de Budapest), que en algunos casos es pertinente en materia de protección de la privacidad. Los esfuerzos de Costa Rica por combatir las prácticas comerciales fraudulentas y engañosas a través de las fronteras se discuten en el informe independiente sobre Política de los Consumidores en Costa Rica, el cual destaca las dificultades que enfrentan los investigadores costarricenses para obtener de sus homólogos en el extranjero y del sector privado información confiable, oportuna y relevante. En este sentido, se espera que la reciente ratificación de la Convención de Budapest mejorará la capacidad de Costa Rica para obtener pruebas en investigaciones relativas a protección de datos que tengan un componente criminal, y que de esta manera ayude a enfrentar las limitaciones jurisdiccionales.

### **12.3. Seguimiento y evaluación**

La PRODHAB publica un informe anual sobre sus actividades y las consultas procesadas por la Agencia están disponibles en <http://www.prodhab.go.cr/resoluciones/>. Si bien la PRODHAB aún no cuenta con los medios o las herramientas para evaluar o darle seguimiento a la efectividad de la Ley N° 8968 y su reglamento, la Agencia está desarrollando una metodología que le permitirá hacerlo. Su publicación está prevista para finales de 2017.

### **12.4. Valoración y recomendaciones**

***Recomendación del Consejo relativa a las directrices que rigen la protección de la privacidad y los flujos transfronterizos de datos personales [OCDE/LEGAL/0352, en su versión vigente; Recomendación del Consejo relativa a la cooperación transfronteriza para la aplicación de las leyes de protección de la privacidad [OCDE/LEGAL/0188]; Declaración sobre flujos de datos transfronterizos [OCDE/LEGAL/0216]***

El régimen de privacidad de Costa Rica está constituido por un marco jurídico y regulatorio integral cuya base es la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 8968), ley que abarca los principios básicos de las directrices de la OCDE en materia de privacidad. La PRODHAB aplica la ley de privacidad de Costa Rica dentro de los límites de sus facultades actuales y lleva a cabo campañas de sensibilización sobre privacidad y protección de datos personales. Los flujos transfronterizos de datos personales no están restringidos. Si bien el régimen de privacidad de Costa Rica aún es incipiente y la agencia a cargo de la protección de los datos (PRODHAB) comenzó a funcionar a mediados de 2014, el país participa en esta materia a escala internacional a través de la Red Iberoamericana de Protección de Datos y planea ampliar sus compromisos internacionales. La PRODHAB prevé completar su estrategia de privacidad a finales de 2017. La estrategia reflejará un enfoque coordinado entre diferentes órganos gubernamentales.

#### ***Recomendaciones***

- Finalizar la estrategia de privacidad de la PRODHAB de manera que refleje un enfoque coordinado entre diferentes órganos gubernamentales.
- Desarrollar e implementar metodologías de seguimiento y evaluación de las actividades de protección de datos que sirvan para fundamentar las políticas;
- Adoptar las medidas apropiadas para facilitar aún más la cooperación transfronteriza en la aplicación de las leyes de privacidad.

## 13. LA GOBERNANZA DE DATOS DE SALUD

### 13.1. Políticas

#### *Marco jurídico*

La juventud del marco jurídico y regulatorio de Costa Rica permite desarrollar procesos de gobernanza de los datos de salud:

- La Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (N° 8968) de 2011 y su Reglamento (detallado en este informe en la Sección 12);
- La Ley de Derechos y deberes de las personas usuarias de los servicios de salud públicos y privados (N° 8239), promulgada en 2013, creó una instancia general, la Auditoria General de Servicios de Salud, así como instancias particulares para los establecimientos de salud conocidas como Contralorías de Servicios de Salud;
- La Ley Reguladora de Investigación Biomédica (N° 9234), promulgada en 2014, creó el Consejo Nacional de Investigación en Salud (CONIS), a cargo de supervisar los Comités Ético-Científicos en las entidades que realizan investigación biomédica.
- La Ley del Expediente Digital Único de Salud (N° 9162), promulgada en 2013, establece las bases normativas para el desarrollo de un Expediente Digital Único de Salud (EDUS) que incluye aspectos de calidad, seguridad de datos, accesibilidad y soluciones tecnológicas para su desarrollo. Esta ley debe estar implementada antes de septiembre de 2018 y es parte del Plan Nacional de Desarrollo 2015-2018 (PND) que define las prioridades de la Administración actual.
- El *Reglamento sobre el uso de estándares para datos de la Salud en Atención de Pacientes* (Decreto Ejecutivo N° 39652-S-MICIT), promulgado en febrero de 2016.
- El *Reglamento del Consentimiento Informado en la Práctica Asistencial en la Caja Costarricense de Seguro Social (CCSS, promulgado por la CCSS en 2012.*

#### *Responsabilidades y facultades*

La PRODHAB es el órgano principal a cargo de la aplicación de la ley de protección de datos personales de Costa Rica y su meta es proteger los derechos de las personas titulares de los datos. La PRODHAB supervisa las actividades de los responsables de datos cuando procesan datos personales, monitorea la legalidad del procesamiento de datos personales de los controladores de datos del sector público y privado, examina las reclamaciones y notificaciones recibidas de personas y realiza inspecciones preventivas por iniciativa propia. La PRODHAB también supervisa las actividades de procesamiento de datos personales en actividades de investigación y establece los requisitos generales de las medidas de protección de datos organizativos y técnicos.

El Ministerio de Salud lidera la formulación e implementación de las políticas de salud. La Caja Costarricense de Seguro Social (CCSS) es la institución encargada de implementar la Ley N° 9162 de 2013 sobre el Expediente Digital Único de Salud.

El Consejo Nacional de Investigación en Salud (CONIS) es el órgano independiente, multidisciplinario y multisectorial establecido por la Ley N° 9234 de 2014 que regula,

supervisa y monitorea la investigación biomédica a escala nacional. El CONIS tiene la autoridad para acreditar, registrar y supervisar los comités ético-científicos multidisciplinares (CEC) que debe establecer cada entidad que realice investigaciones biomédicas. El CONIS también acredita a investigadores y entre sus otras funciones están la inspección, el mantenimiento de registros y el inicio de procesos administrativos y judiciales.

### 13.2. Implementación

Costa Rica está trabajando para desarrollar e implementar un marco nacional de gobernanza de datos de salud que asegure la privacidad y, al mismo tiempo, permita el uso de datos de salud cuando hacerlo sea de interés público. Los datos de salud se utilizan para fines de interés público relacionados con la salud con el objetivo de mejorar la calidad de la atención de salud, administrar de manera eficiente los recursos sanitarios y contribuir al progreso general de la ciencia y la medicina.

Cabe señalar que la discusión del Comité de Salud de la OCDE sobre las políticas de salud en Costa Rica y la finalización del examen de adhesión del Comité de Salud precedió a la adopción de la *Recomendación del Consejo relativa a la Gobernanza de Datos de Salud* [[OCDE/LEGAL/0433](#)]. No obstante, el Comité de Salud determinó que, en general, el sector salud de Costa Rica muestra "un impresionante grado de coordinación intersectorial a nivel nacional, junto con un diálogo efectivo entre los usuarios y los administradores de los servicios de salud orientado a impulsar la mejora de los servicios a nivel local; además de innovación en torno a las funciones profesionales y el uso de las TIC de los que otros sistemas de salud podrían aprender".

Costa Rica aspira a garantizar la interoperabilidad efectiva de la información en el sector de la salud. El Reglamento sobre el Uso de Estándares para Datos de la Salud en Atención de Pacientes (Decreto Ejecutivo N° 39652-S-MICIT) de febrero de 2016 regula "*la utilización de las normas de información en salud y la interoperabilidad entre los sistemas de información de Salud de Costa Rica, entre los diferentes niveles de gestión, primer nivel, segundo nivel y tercer nivel, sistemas públicos, privados y aseguradoras de salud*". El Reglamento crea una comisión encargada de poner en práctica el decreto y desarrollar los estándares necesarios; en ella participan instituciones públicas, proveedores de servicios públicos y privados y el Colegio de Médicos y Cirujanos (Artículo 2). Además, establece un período de dos años (hasta febrero de 2018) para que las instituciones del sector de la salud cumplan con los estándares de interoperabilidad. Estos estándares incluyen la Norma INTE/ISO/HL7 27931:2016, un protocolo para el intercambio electrónico de datos de atención médica.<sup>50</sup> Promover "*la interoperabilidad de la información, el procesamiento, la confidencialidad, la seguridad y el uso de estándares y protocolos entre las distintas entidades del sector salud*" también es un objetivo de la Ley de Expediente Digital Único de Salud (N° 9162) promulgada en 2013.

Costa Rica evaluó recientemente la capacidad de los sistemas de datos de salud del sector público que se utilizan para procesar los datos personales de salud en servicio y protección del interés público. La Contraloría General de la República (CGR) revisó el desarrollo del Expediente Digital Único de Salud gestionado por la Caja Costarricense de Seguro Social (CCSS) y publicó un informe al respecto en 2016.

La legislación nacional prevé que el procesamiento de datos personales de salud requiere el consentimiento informado y que se les debe proporcionar información clara a las personas respecto de la recolección, los objetivos, los beneficios y la base jurídica del procesamiento de sus datos personales de salud y las alternativas apropiadas. La Ley N° 8968 considera los datos de naturaleza biomédica y genética como "datos sensibles", es decir, como "información relativa al fuero íntimo de la persona" (artículo 3 e) y prohíbe su procesamiento. En el caso de la investigación biomédica, la Ley 9234 establece los requisitos del consentimiento informado (artículo 10), así como para la información de investigaciones clínicas (artículo 11).

Existen alternativas y exenciones legales para solicitar el consentimiento. Por ejemplo, la Ley 8968 estipula que no se requiere consentimiento cuando sea necesario *"para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta, asimismo, a una obligación equivalente de secreto."* (artículo 9 d). La Ley 8239 sobre Derechos y deberes de las personas usuarias de los servicios de salud públicos y privados estipula el derecho de *"[h]acer que se respete el carácter confidencial de su historia clínica y de toda la información relativa a su enfermedad salvo cuando, por ley especial, deba darse noticia a las autoridades sanitarias"*.

La Ley N° 8968 define a cuáles personas se les considera responsables de la gestión de los datos personales (artículo 3). El Reglamento a la Ley 8968, creado por el Decreto Ejecutivo N° 37554, proporciona controles y salvaguardas mediante el establecimiento de las medidas de seguridad que deben seguirse en el manejo y procesamiento de datos personales.

Costa Rica cuenta con procedimientos de revisión y aprobación del uso de datos personales de salud en investigaciones y otros fines de interés público relacionados con la salud. Por ejemplo, el CONIS acredita, registra y supervisa los Comités Ético-Científicos (CEC) multidisciplinarios que se establecen en cada entidad en donde se realizan investigaciones biomédicas. El CONIS también acredita a investigadores y entre sus otras funciones están la inspección, el mantenimiento de registros y el inicio de procesos administrativos y judiciales.

Costa Rica maximiza el potencial y promueve el desarrollo de tecnología con el sector salud de Costa Rica utilizando y mejorando herramientas para recolectar y procesar datos de salud de manera continua, los cuales adapta de acuerdo con las tendencias mundiales, utilizando tecnologías cada vez más sofisticadas y centrándose cada vez más en la seguridad de la información y la privacidad.

La PRODHAB realiza actividades de educación y sensibilización, desarrollo de habilidades y prevención, y promueve medidas técnicas que ayuden a proteger la privacidad en Costa Rica. Consulta con las personas titulares de datos, los controladores y procesadores de datos y otros con respecto a la protección de los datos personales y la privacidad, incluido el procesamiento de datos personales con fines científicos y de investigación médica.

## Evaluación

### ***Recomendación del Consejo relativa a la gobernanza de datos de salud [OCDE/LEGAL/0433]***

Costa Rica reconoce la importancia de equilibrar la necesidad de proteger los datos personales y al mismo tiempo permitir su disponibilidad e intercambio para fines de salud pública, atención médica e investigación, y está desarrollando su sistema de gobernanza de datos de salud de conformidad con estos principios.

## 14. LA PROTECCIÓN EN LÍNEA DE LOS NIÑOS Y NIÑAS

### 14.1. Políticas

El enfoque de las políticas para la protección de la niñez en línea en Costa Rica se articula en torno a cuatro acciones principales: *i)* fortalecer el marco regulatorio; *ii)* fortalecer la coordinación interinstitucional; *iii)* identificar e implementar proyectos que promueven una cultura de protección en línea; y *iv)* apoyar la investigación y la evaluación de los impactos de los planes nacionales.

Las políticas en áreas relacionadas como la protección de datos, la investigación penal, la educación, la distribución de películas y juegos de computadora también incorporan la protección en línea de los niños y niñas.

#### *Marco jurídico y regulatorio*

Desde que firmó la Convención sobre los Derechos del Niño en 1990, Costa Rica se ha comprometido formalmente a respetar los derechos de las personas menores de edad, a quienes considera personas sujetas de derechos. Varias leyes nacionales e internacionales responden a este compromiso y constituyen el Sistema Nacional de Protección Infantil, que, a través de la participación de una serie de actores institucionales, procura coordinar las acciones para la protección de los derechos civiles, políticos, económicos, sociales y culturales que requiere esta población.

Costa Rica ha aprobado una serie de leyes que protegen a la niñez: la Ley contra la Violencia Doméstica (1996), la Ley General de Protección a la Madre Adolescente (1997), la actualización de la gestión del Patronato Nacional de la Infancia (PANI) (1997), el establecimiento del Código de la Niñez y la Adolescencia (1998) y la Ley contra la Explotación Sexual de Personas Menores de Edad (1999).

Sin embargo, la base jurídica de la protección de la niñez en línea en Costa Rica la provee, principalmente, la Ley de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y Otros Medios Electrónicos (N° 8934, del 27/04/2011).

Las disposiciones de esta ley se extendieron a los cibercafés el 23 de marzo de 2012 mediante el Decreto Ejecutivo N° 31763, Reglamento de Control y Regulación de Locales que ofrecen Servicio Público de Internet.

Además, la Ley N° 9135 de 2013 modificó el Código Penal con la adición del Artículo 167 bis (Seducción o encuentros con menores por medios electrónicos), que sanciona con dos o tres años de prisión a quien, a sabiendas y con conocimiento del carácter del material, establece una comunicación que incluya contenido pornográfico por medios digitales con una persona menor de edad.

El Decreto Ejecutivo N° 31764 del 26/04/2004 introdujo el Reglamento de Funcionamiento de las Salas de Videojuegos o Juegos Cibernéticos y la Clasificación de los Juegos según el Nivel de Violencia, que dispone normas para su etiquetado y clasificación de acuerdo con las normas internacionales.

#### *Responsabilidades y facultades*

Varios ministerios y agencias participan en el desarrollo de políticas sobre temas relacionados con la protección en línea de los niños y niñas. El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el órgano rector en el campo de las tecnologías de la información y la comunicación (TIC) y coordina las actividades de la Comisión Nacional de Seguridad en Línea establecida en 2010 por el Decreto Ejecutivo N° 36274. El objetivo de la Comisión es promover el uso seguro, significativo y productivo de

las TIC por parte de las personas menores de edad y empoderar a familias y niños y niñas a través de programas educativos específicos. El Ministerio de Educación Pública (MEP) y el Ministerio de Cultura y Juventud (MCJ) también son miembros de la Comisión Nacional de Seguridad en Línea.

El Patronato Nacional de la Infancia (PANI) de Costa Rica, establecido en 1930, es el órgano responsable de la implementación de políticas para niños y niñas y adolescentes; esto incluye planes, programas y proyectos para promover y garantizar los derechos y el desarrollo integral de las personas menores de edad y sus familias., con la participación de instituciones estatales y otros actores sociales. Junto con la sociedad civil, el PANI participa en acciones para salvaguardar la integridad física y emocional de los niños y niñas y adolescentes que se exponen a situaciones de alto riesgo y cuyos progenitores no pueden cuidarlos adecuadamente.

El Consejo Nacional de la Niñez y la Adolescencia, un organismo creado por la Ley N° 7739 en 1998, está adscrito al Poder Ejecutivo y provee un espacio para el debate, la consulta y la coordinación entre el Ejecutivo, las instituciones estatales descentralizadas y las organizaciones comunitarias representativas. Tiene el poder de garantizar que la formulación y la implementación de políticas públicas sean consistentes con la visión del país de un marco jurídico integral para la protección de los derechos de las personas menores de edad, de conformidad con el Código de la Niñez y la Adolescencia (CNA) y de acuerdo con los principios establecidos.

La Comisión Nacional Contra la Explotación Sexual Comercial de Niños, Niñas y Adolescentes (CONACOES) también participa en la prevención de la explotación sexual en línea de niños, niñas y adolescentes. La CONACOES pertenece al Consejo Nacional de la Niñez y la Adolescencia. Recibe su legitimidad del Patronato Nacional de la Infancia.

Las organizaciones no gubernamentales (ONG), las empresas y la sociedad civil desempeñan una función central en el desarrollo y la implementación de políticas y están representadas tanto en el Consejo Nacional de la Niñez y la Adolescencia como en la Comisión Nacional de Seguridad en Línea. Las ONG más importantes de la Comisión Nacional de Seguridad en Línea son la Fundación Paniamor y la Fundación Omar Dengo, ambas creadas en 1987 como entidades sin fines de lucro.

El Ministerio de Relaciones Exteriores designó en 2005 a la Fundación Paniamor como la institución con mejores prácticas en cooperación internacional. Su misión es catalizar cambios duraderos en la calidad de vida de los niños y niñas promover el cumplimiento de las leyes que protegen los derechos de la niñez en Costa Rica.

La Fundación Omar Dengo tiene como objetivo desarrollar y mejorar la calidad de la educación a través de la informática y la aplicación de nuevas tecnologías en el sistema educativo costarricense.

## 14.2. Implementación

### *Medidas no regulatorias*

El MICITT y el MEP desempeñan una función importante en la realización de campañas de sensibilización del público y de actividades educativas. Estos órganos ayudan a coordinar y promover campañas de prevención para sensibilizar a los progenitores y sus hijos e hijas sobre comportamientos responsables, capacitar a funcionarios y crear protocolos, manuales e instrumentos basados en la web dirigidos a padres y madres, docentes y niños y niñas.

Durante el período que abarca el informe, las actividades coordinadas por el MICITT incluyeron:

- "*Crianza tecnológica*" ([www.crianzatecnologica.org](http://www.crianzatecnologica.org)), plataforma desarrollada en colaboración con la Fundación Paniamor. Se trata de una plataforma basada en la web para madres y padres, docentes y personas responsables que brinda orientación sobre el uso seguro de la internet y las tecnologías móviles. (<http://crianzatecnologica.paniamordigital.org/>)
- Campañas de sensibilización del público a través de redes sociales para promover la protección en línea en colaboración con empresas de tecnologías móviles e instituciones públicas. En 2016, en el marco del Día de la Internet Segura, el MICITT organizó una teleconferencia que incluyó a actores del MICITT, la Universidad Estatal a Distancia (UNED), la Fundación Paniamor, NIC-CR y Chicos.NET.

Durante el período que abarca el informe, las actividades coordinadas por el MEP incluyeron:

- La implementación de una estrategia nacional llamada "Tecnoaprender", que promueve el desarrollo de habilidades digitales y da consejos a niños y niñas, adolescentes, docentes y padres y madres sobre el uso seguro y productivo de las tecnologías digitales.
- Seminarios y sesiones de capacitación para especialistas, docentes, bibliotecarios y capacitadores, en cooperación con la Fundación Omar Dengo; por ejemplo, el "Programa Nacional de Informática Educativa", cuyo objetivo principal es desarrollar capacidades en el uso y la apropiación de tecnologías digitales.

### ***Aplicación de la ley***

El MICITT y el PANI son responsables de promover el diseño, la implementación y la ejecución de políticas para la protección de la niñez de acuerdo con la legislación. El regulador de la industria de telecomunicaciones en Costa Rica, la Superintendencia de Telecomunicaciones (SUTEL), es la entidad responsable de implementar las disposiciones relativas a las regulaciones sobre contenido dañino en internet y otros medios electrónicos. El Poder Ejecutivo es responsable de coordinar las políticas y garantizar el cumplimiento.

Cuando el PANI tiene conocimiento de una situación que viola los derechos de una o más personas menores de edad a través de medios digitales en internet, coordina con las instituciones pertinentes y remite el caso a los tribunales. Se basa en las disposiciones del artículo 111 del Código de la Niñez y la Adolescencia.

Costa Rica aprobó en 2011 la Convención Interamericana sobre Asistencia Mutua en Materia Penal (Ley N° 9006). Esta convención multilateral compromete a los signatarios a proveer asistencia mutua en investigaciones penales y procedimientos judiciales, incluidos todos los delitos relacionados con la informática que involucren a personas menores de edad.

### **14.3. Seguimiento y evaluación**

En Costa Rica no existe un proceso formalmente establecido para medir y evaluar regularmente la efectividad de las políticas e iniciativas. Sin embargo, los avances y las necesidades que van surgiendo son monitoreados a través de encuestas e investigaciones ad hoc realizadas por centros académicos y otras instituciones.

Como ejemplo, en 2013 la Fundación Paniamor y el Instituto de Investigaciones Psicológicas (IIP) de la Universidad de Costa Rica, con el apoyo de MICITT-CONICIT, llevaron a cabo un proyecto de investigación sobre el uso de teléfonos inteligentes, tabletas e internet entre niños y niñas de 10 a 13 años del Área Metropolitana de Costa Rica. Los resultados indicaron que el 84% de los niños y niñas entre 10 y 12 años tenían teléfono celular y el 67% accedía a internet desde su teléfono. El estudio también mostró que la

mayoría de los niños y las niñas usan sus teléfonos celulares para entretenerse. Es decir, lo usan para juegos, redes sociales y YouTube.

El estudio aportó información sobre el nivel de uso de tecnologías digitales por parte de los niños y niñas y destacó las brechas en la conciencia del riesgo y la necesidad de una mayor educación y capacitación de los adultos y cuidadores para apoyar y guiar a las personas menores de edad en el uso de tecnologías digitales. En 2016 esto llevó al MICITT a apoyar a la Fundación Paniamor en el establecimiento del programa *Crianza Tecnológica*.

#### 14.4. Valoración y recomendaciones

##### ***Recomendación del Consejo relativa a la protección en línea de los niños y niñas [OCDE/LEGAL/0389]***

El principal objetivo de las políticas de Costa Rica para la protección de los niños y niñas en línea es extender a internet la protección que se les da fuera de línea. Los marcos jurídicos sobre protección infantil y comunicaciones reflejan valores fundamentales e incluyen regulaciones específicas para la protección de las niñas y niños en línea. En esta área, las principales responsabilidades recaen en el Ministerio de Ciencia, Tecnología y Telecomunicaciones, el Ministerio de Educación Pública y el Patronato Nacional de la Infancia. La Fundación Paniamor y la Fundación Omar Dengo son muy activas en la implementación de una serie de medidas para empoderar y educar a los niños y las niñas, las personas adolescentes, docentes, madres y padres y para la concienciación a través de los medios. La cooperación internacional se produce principalmente a escala regional; por ejemplo, a través de la participación de Costa Rica en la Convención Interamericana sobre Asistencia Mutua en Materia Penal. Establecida en 2010, la Comisión Nacional de Seguridad en Línea es un buen medio para mejorar la coordinación de los diferentes actores que participan en el desarrollo y la implementación de políticas para la protección en línea de los niños y niñas.

##### ***Recomendación***

- Mejorar el seguimiento y la medición regulares de la evolución de la alfabetización digital de los niños y niñas y promover el crecimiento de una base empírica y analítica sólida para el desarrollo y la implementación de políticas basadas en la evidencia.



## Notas

1 Según el MICITT, las áreas no rentables corresponden a áreas rurales, áreas remotas y territorios indígenas en condición de vulnerabilidad social, económica y cultural.

2 La participación privada en el capital social de las empresas constituidas o adquiridas por el ICE se limita al 49%; por lo tanto, el control de las empresas sigue siendo público.

3 La Estrategia señala que, actualmente, el único programa de grado en seguridad de la información en universidades de Costa Rica es privado. Tiene apoyo de empresas multinacionales.

4 Por ejemplo, la tercerización de las operaciones de red puede crear riesgos si los proveedores de servicios no aceptan niveles mínimos de prestación de servicios, incluido un tiempo de respuesta aceptable y medidas de seguridad mínimas.

5 Hasta ahora han emitido lo siguiente: "Política de Certificados para la jerarquía nacional de certificadores registrados", "Política de sellado de tiempo", "Directrices para las autoridades de registro", "Características de cumplimiento para las autoridades de registro (AR) de la Jerarquía Nacional de Certificadores Registrados".

6 Plan Nacional de Desarrollo "Alberto Cañas Escalante" [Plan Nacional de Desarrollo 2015-2018](#)  
7 Estrategia Nacional de Gobierno Abierto (ENGA) (2015). [Estrategia Nacional de Gobierno Abierto: Gobierno abierto](#), <http://gobiernoabierto.go.cr/>

8 Decreto de Apertura de Datos, del 12 de mayo de 2017.

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=84004&nValor3=108193&param2=1&strTipM=TC&IResultado=1&strSim=simp](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=84004&nValor3=108193&param2=1&strTipM=TC&IResultado=1&strSim=simp)

9 Decreto de Transparencia y Acceso a la Información Pública, 2 de junio de 2017.

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=84166&nValor3=108486&param2=1&strTipM=TC&IResultado=1&strSim=simp](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=84166&nValor3=108486&param2=1&strTipM=TC&IResultado=1&strSim=simp)

10 Constitución Política de la República de Costa Rica (2015),

Artículos 27 y 30)

[http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=871&strTipM=TC](http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=871&strTipM=TC)

11 Decreto Ejecutivo N° 38994-MP-PLAN-MICITT, Fomento del Gobierno Abierto en la Administración Pública y Creación de la Comisión Nacional para un Gobierno Abierto (2015).

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=79442&nValor3=100459&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=79442&nValor3=100459&strTipM=TC)

12 Ley de Protección de la Persona frente al Tratamiento de sus Datos personales (2011), Ley N° 8968, PRODHAB, Ministerio de Justicia y Paz, artículos 4, 5, 6 y 16.

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=0&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=0&strTipM=TC). Para ver las actividades actuales consultar: Agencia de

Protección de Datos de los Habitantes <http://www.prodhhab.go.cr/>. Véase también la Ley de Regulación del

Derecho de Petición (2013), Ley N° 9097, [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=74427&nValor3=91901&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74427&nValor3=91901&strTipM=TC).

13 Véase el sitio web de Gobierno Abierto: [www.gobiernoabierto.go.cr](http://www.gobiernoabierto.go.cr) y OCDE (2016), Gobierno Abierto en Costa Rica. <http://gobiernoabierto.go.cr/wp-content/uploads/2016/04/Highlights-OG-Costa-Rica-V3-080416.pdf>

14 Borrador disponible en: [www.gobiernoabierto.go.cr](http://www.gobiernoabierto.go.cr)

15 Véase <https://www.poder-judicial.go.cr/salaconstitucional/index.php/informacion/700-13-015183>, para otros ejemplos ver <http://www.nacion.com/etiqueta/prodhhab/> y <http://www.elfinancierocr.com/etiqu/prodhhab/>

- 16 Ley General de Telecomunicaciones N° 8642. [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=91176&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=91176&strTipM=TC)
- 17 Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, N° 8220, artículos 1 y 5. [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=48116&nValor3=86446&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=48116&nValor3=86446&strTipM=TC)
- 18 Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2018: <http://www.micit.go.cr/images/Telecomunicaciones/pndt/PNDT-2015-2021.pdf>
- 19 Sala Constitucional. <http://sitios.poder-judicial.go.cr/salaconstitucional/>. Contraloría General de la República. <http://www.cgr.go.cr/>
- 20 Código Penal (2014), Ley N° 4573, artículos 293 y 294. [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=98548&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=98548&strTipM=TC) Abarca secretos de estado relacionados con la seguridad interna o externa, y la información obtenida como parte del puesto de trabajo de un individuo. Código Procesal Penal (2014), Ley N° 7594, artículo 206. [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_textocompleto.aspx?param1=NRTC&nValor1=1&nValor2=41297&nValor3=101880&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_textocompleto.aspx?param1=NRTC&nValor1=1&nValor2=41297&nValor3=101880&strTipM=TC) Obligación de divulgar información personal confidencial si el interesado está de acuerdo.
- 21 La información y los datos se pueden encontrar directamente en: <http://datosabiertos.presidencia.go.cr/home>
- 22 Véase también: PRODHAB *op. cit.*; Constitución Política de la República de Costa Rica, artículos 27 y 30, *op. cit.*; Ley de la Jurisdicción Constitucional, N° 7135, artículo 32.
- 23 Ley sobre Derechos de Autor y Derechos Conexos (Ley N° 6683). [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_norma.aspx?param1=NRM&nValor1=1&nValor2=3396&nValor3=80724&strTipM=FN](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=3396&nValor3=80724&strTipM=FN)
- 24 Oficina de Transparencia de la Presidencia: <http://presidencia.go.cr/directrices-presidenciales/>
- 25 Política sobre el uso de Internet y el desarrollo de sitios web en instituciones públicas, Directriz N° 040, MICITT (28 de abril de 2005). [http://www.archivonacional.go.cr/pdf%5Cmarco\\_juridico\\_2016%5Cdirectrices%5Cdirectriz\\_sitios\\_web.pdf](http://www.archivonacional.go.cr/pdf%5Cmarco_juridico_2016%5Cdirectrices%5Cdirectriz_sitios_web.pdf)
- 26 [www.gobiernoabierto.go.cr/seguimiento/](http://www.gobiernoabierto.go.cr/seguimiento/) Véase también OECD (2016), Open Government in Costa Rica. <http://gobiernoabierto.go.cr/wp-content/uploads/2016/04/Highlights-OG-Costa-Rica-V3-080416.pdf>
- 27 La matriz de evaluación de la ENGA está disponible en el anexo del documento en línea, a partir de la página 30: [http://gobiernoabierto.go.cr/estrategia/Los\\_resultados\\_de\\_2015\\_y\\_2016\\_estan\\_disponibles\\_en](http://gobiernoabierto.go.cr/estrategia/Los_resultados_de_2015_y_2016_estan_disponibles_en)
- [http://www.dhr.go.cr/red\\_de\\_transparencia/indice\\_de\\_transparencia\\_del\\_sector\\_publico.aspx](http://www.dhr.go.cr/red_de_transparencia/indice_de_transparencia_del_sector_publico.aspx)
- 28 Eje de transparencia y acceso a la información en la estrategia nacional de gobierno abierto <http://gobiernoabierto.go.cr/eje-de-transparencia-y-acceso-a-la-informacion/>
- 29 El Índice de Transparencia del Sector Público de la Defensoría de los Habitantes está disponible en: [http://www.dhr.go.cr/red\\_de\\_transparencia/indice\\_de\\_transparencia\\_del\\_sector\\_publico.aspx](http://www.dhr.go.cr/red_de_transparencia/indice_de_transparencia_del_sector_publico.aspx)
- El informe de autoevaluación de 2016 está en: <http://gobiernoabierto.go.cr/documentos/>
- 30 Informe de la Asociación de Gobierno Abierto: [https://www.opengovpartnership.org/sites/default/files/Costa-Rica\\_Progress\\_2015-2017\\_comments-recd.pdf](https://www.opengovpartnership.org/sites/default/files/Costa-Rica_Progress_2015-2017_comments-recd.pdf)
- 31 Acuerdo N° ETCPS-011-2016, Equipo Técnico del Consejo Presidencial Social. La Comisión incluye: El Ministerio de Ambiente y Energía (MINAE); Viceministerio de Telecomunicaciones, Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT); Instituto Nacional de Aprendizaje (INA); Ministerio de Salud; y representantes académicos.
- 32 Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) (2015), Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021: Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021: "Costa Rica una sociedad conectada", San José, Costa Rica.
- 33 Ley para la Gestión Integral de Residuos, Ley N° 8839, Casa Presidencial, Ministerio de Salud y Ministerio de Ambiente y Energía, 13 de julio de 2010. Los residuos de manejo especial "*son aquellos que por su composición, necesidades de transporte, condiciones de almacenaje, formas de uso o valor de recuperación, o por una combinación de esos, implican riesgos significativos a la salud y degradación sistemática de la calidad del ecosistema, por lo que requieren salir de la corriente normal de residuos ordinarios.*"

34 Decreto Ejecutivo N° 37658-MINAET (2013) (*Establece el Sistema Nacional de Información Ambiental (SINIA) y reforma el Decreto Ejecutivo N° 29540 "Constituye el Centro Nacional de Información Geoambiental como un órgano de la Dirección General de Hidrocarburos del Ministerio de Ambiente y Energía"*).

35 Ministerio de Ambiente y Energía (2015), Plan Nacional de Energía 2015-2030

36 Ver nota 1, *op. cit.*

37 Este análisis se basa en las recomendaciones contenidas en la *Recomendación del Consejo relativa a las tecnologías de información y comunicación y el medio ambiente* [OECD/LEGAL/0380].

38 Decreto Ejecutivo N° 35933-S: Reglamento para la Gestión Integral de los Residuos Electrónicos

[https://www.imprentanacional.go.cr/pub/2010/05/05/COMP\\_05\\_05\\_2010.html#\\_Toc260740991](https://www.imprentanacional.go.cr/pub/2010/05/05/COMP_05_05_2010.html#_Toc260740991)

39 <https://www.grupoice.com/wps/portal/ICE/AcercaDelGrupoICE/Laboratorios/LMVE>

40 <https://www.grupoice.com/wps/portal/ICE/Electricidad/ProyectosEnergéticos/ProgramaBioGas>

41 [http://www.conicit.go.cr/boletin/boletin51/patente\\_TEC.shtml](http://www.conicit.go.cr/boletin/boletin51/patente_TEC.shtml)

42 Política Nacional de Compras Sustentables (2015).

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=80785&nValor3=102645&param2=1&strTipM=TC&lResultado=2&strSim=simp](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=80785&nValor3=102645&param2=1&strTipM=TC&lResultado=2&strSim=simp)

Dr. Alfonso Carro Zúñiga, Objetivo 6, p. 27. <http://www.ina.ac.cr/Documentos.html>

44 Avance SGA, INA II Semestre 2015 y Resumen Sistema de Gestión Ambiental del INA, junio de 2016. Datos del 2016 provistos por el INA.

45 Decreto Ejecutivo N° 36499-S-MINAET.

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=70199&nValor3=84619&param2=1&strTipM=TC&lResultado=7&strSim=simp](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70199&nValor3=84619&param2=1&strTipM=TC&lResultado=7&strSim=simp)

46 1<sup>er</sup> Informe del Estado del Teletrabajo en Costa Rica <http://ciidtt.org/sites/default/files/2017-04/PrimerInformeTeletrabajo.pdf>

47 Decreto Ejecutivo N° 39310-H-MINAE-MEIC-MTSS (2015): Política Nacional de Compras Públicas Sustentables y Creación del Comité Directivo Nacional de Compras Sustentables)

[http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?Param1=NRTC&nValor1=1&nValor2=80785&nValor3=102645&strTipM=TC](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?Param1=NRTC&nValor1=1&nValor2=80785&nValor3=102645&strTipM=TC)

48 [https://www.hacienda.go.cr/comprared/Manual\\_Compras\\_Verdes.pdf](https://www.hacienda.go.cr/comprared/Manual_Compras_Verdes.pdf)

49 El salario base mensual de un asistente judicial, de acuerdo con la Ley de Presupuesto de la República de Costa Rica.

50 El artículo 17 del Decreto Ejecutivo N° 39652-S-MICIT contiene el Estándar INTE/ISO/HL7 27931:2016 Estándar de intercambio de datos -HL7 Versión 2.5, un protocolo de aplicación para el intercambio electrónico de datos de atención de salud, publicado el 13 de enero de 2017. Este estándar fue emitido por el Instituto de Normas Técnicas de Costa Rica (INTECO), la entidad nacional a cargo de la normalización en Costa Rica. Esta norma corresponde a la norma internacional ISO/HL7 27931:2009.